NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FMCW RADAR JAMMING TECHNIQUES AND ANALYSIS

by

Hung-Ruei Chen

September 2013

Thesis Advisor:	Phillip Pace
Co-Advisor:	David Garren
Second Reader:	Edward Fisher

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2013	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
FMCW Radar Jamming Techniques And Analysis	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School Monterey, CA 93943-5000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Frequency-Modulated Continuous-Wave (FMCW) radar is a type of Low Probability of Intercept radar system that is being heavily investigated in the military. Not only is its transmission difficult to be detected by enemy intercept receivers, but FMCW radar has the inherent capability of increasing coherent signal power while suppressing noise power during its receive signal processing. This thesis investigates the jamming effectiveness of selected jamming waveforms by injecting the interfering signals into the Lab-Volt Radar Training System (LVRTS). The jamming effect is evaluated based on the change in beat frequency due to the jamming. Due to the hardware limitations of the LVRTS, a MATLAB simulation model is also constructed for advanced electronic attack testing. The MATLAB model emulates the FMCW emitter digital signal processing response to coherent and non-coherent jamming signals under an anti-ship capable missile scenario. The simulation output is the target range and range rate, whose error measures quantify the jamming effectiveness. From the standpoint of electronic warfare, related subjects such as electronic warfare support measures and FMCW electronic protection are also discussed.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**103**	

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
FMCW RADAR JAMMING TECHNIQUES AND ANALYSIS

5. FUNDING NUMBERS

6. AUTHOR(S) Hung-Ruei Chen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Frequency-Modulated Continuous-Wave (FMCW) radar is a type of Low Probability of Intercept radar system that is being heavily investigated in the military. Not only is its transmission difficult to be detected by enemy intercept receivers, but FMCW radar has the inherent capability of increasing coherent signal power while suppressing noise power during its receive signal processing. This thesis investigates the jamming effectiveness of selected jamming waveforms by injecting the interfering signals into the Lab-Volt Radar Training System (LVRTS). The jamming effect is evaluated based on the change in beat frequency due to the jamming. Due to the hardware limitations of the LVRTS, a MATLAB simulation model is also constructed for advanced electronic attack testing. The MATLAB model emulates the FMCW emitter digital signal processing response to coherent and non-coherent jamming signals under an anti-ship capable missile scenario. The simulation output is the target range and range rate, whose error measures quantify the jamming effectiveness. From the standpoint of electronic warfare, related subjects such as electronic warfare support measures and FMCW electronic protection are also discussed.

14. SUBJECT TERMS FMCW Radar, LPI, Jamming, Electronic Warfare			**15. NUMBER OF PAGES** 103
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FMCW RADAR JAMMING TECHNIQUES AND ANALYSIS

Hung-Ruei Chen
Lieutenant, Taiwan Navy
B.S., Virginia Military Institute, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRONIC WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Hung-Ruei Chen

Approved by: Phillip Pace, PhD
Thesis Advisor

David Garren, PhD
Co-Advisor

Edward Fisher
Second Reader

Dan Boger, PhD
Chair, Department of Information Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Frequency-Modulated Continuous-Wave (FMCW) radar is a type of Low Probability of Intercept radar system that is being heavily investigated in the military. Not only is its transmission difficult to be detected by enemy intercept receivers, but FMCW radar has the inherent capability of increasing coherent signal power while suppressing noise power during its receive signal processing. This thesis investigates the jamming effectiveness of selected jamming waveforms by injecting the interfering signals into the Lab-Volt Radar Training System (LVRTS). The jamming effect is evaluated based on the change in beat frequency due to the jamming. Due to the hardware limitations of the LVRTS, a MATLAB simulation model is also constructed for advanced electronic attack testing. The MATLAB model emulates the FMCW emitter digital signal processing response to coherent and non-coherent jamming signals under an anti-ship capable missile scenario. The simulation output is the target range and range rate, whose error measures quantify the jamming effectiveness. From the standpoint of electronic warfare, related subjects such as electronic warfare support measures and FMCW electronic protection are also discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADC	Analog-to-Digital Converter
ASCM	Anti-Ship Capable Missile
CW	Continuous Wave
DFT	Discrete Fourier Transform
DRFM	Digital Radio Frequency Memory
DSP	Digital Signal Processing
EA	Electronic Attack
EP	Electronic Protection
ES	Electronic Warfare Support
EW	Electronic Warfare
FFT	Fast Fourier Transform
FM	Frequency-Modulated
FMCW	Frequency-Modulated Continuous Wave
GO-CFAR	Greatest of Constant False Alarm Rate
IF	Intermediate Frequency
LPI	Low Probability of Intercept
LVRTS	Lab-Volt Radar Training System
PFA	Probability of False Alarm
RF	Radio Frequency
RGPO	Range-Gate Pull-Off
SNR	Signal-to-Noise Ratio
VGPO	Velocity Gate Pull-Off

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to thank my thesis advisor, Prof. Phillip Pace for the motivation and support he has provided throughout the research. His patience and encouragement gave me the confidence I needed to overcome stumbling blocks during the research. Co-advisors Prof. David Garren and Mr. Edward Fisher's valuable advice on the research approach have greatly enhanced the quality of the thesis. This research could not be completed without the technical support provided by the Radar/EW Lab Director, Mr. Paul Buczynski, and the lab technician, PO2 Edward Montoya. Mrs. Donna Aikins, the loving mother of the office, gave me much advice on writing and formatting. Last but not least, I want to thank Dr. Ming-Jer Huang, who gave me much emotional support in many ways during my stay in Monterey.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Low Probability of Intercept (LPI) radar is the trend of modern radar systems and has been proven effective in modern electronic warfare (EW) operations. Because of its low power, wide bandwidth, frequency variability features, LPI radar is difficult to detect by means of a passive non-cooperative intercept receiver. Among the many variations of LPI radar systems, Frequency-Modulated Continuous Wave (FMCW) radar has not only the ability to avoid detection, but also the inherent resistance to electronic attack (EA) once transmission is detected. Although highly capable, FMCW has a relatively simple structure, which makes it highly applicable for many modern radar systems. Such features attract much interest in FMCW radar, which has become the trend of modern radar development.

FMCW radar is problematic to the enemy in EW due to the fact that its coherent nature and signal processing architecture gives significant processing gain to the radar echo signal, while discriminating non-coherent signals. These features allow the radar transmitter to operate at very low power and avoid interception by enemy electronic support (ES) receivers, and it also suppresses noise and jamming signals. Furthermore, its wideband transmission and power management system gives an additional advantage to FMCW radar against non-cooperative intercept receiver, as it is difficult to be aware of the presence of LPI signal in the radio spectrum among the noise and clutter.

Considering the effectiveness of FMCW radar, jamming techniques that are capable of interfering with FMCW radar have become a subject of high interest. The goal of this research is to evaluate the effectiveness of selected jamming techniques against FMCW radar systems by looking into FMCW signal processing techniques, against which possible jamming techniques are investigated. The research focuses on the jamming phase of EW operation, with extended discussion of detection of LPI radars and possible electronic protection (EP) mechanisms that may be implemented in the FMCW emitter. The research questions can be summarized as:

- Primary Question:
  - What are some of the effective jamming techniques against FMCW?
- Subsidiary Questions:
  - What makes FMCW radar jamming-resistant?
  - What are the ways to increase Jammer-to-Signal Ratio (JSR) at the radar receiver?
  - How can the simulation results be implemented in a real-world EW scenario?

The research includes experiments using the Lab-Volt Radar Training System (LVRTS) as well as MATLAB simulation. LVRTS is a compact radar system that can be configured as FMCW radar and is suitable for operation in a laboratory environment. Using an arbitrary waveform generator, several jamming waveforms can be generated and applied to the LVRTS receiving antenna. The effectiveness of the jamming waveforms is evaluated by observing their influences on the signal beat frequency. The computer simulation is a separate experiment, which includes several MATLAB models that emulate an EW scenario. The radar model reconstructs a typical homodyne FMCW radar signal-processing algorithm. By applying different computer-generated jamming waveforms, the effect of the EA can be visualized in the radar spectrum, and the effectiveness of the EA techniques can be evaluated.

B. LITERATURE REVIEW

FMCW radar jamming has been briefly discussed in many articles and studies. In [1] it is stated that if the modulation period and modulation bandwidth can be determined, then coherent deception jamming is feasible and very effective.

Reference [2] suggests that there are two basic approaches for jamming FMCW radar systems. One approach is to predict the frequency-versus-time characteristics of the signal and use a jammer that will input energy to the receiver at the same frequency as the FM signal that it is attempting to receive. This strategy allows the maximum JSR to be achieved for any given jammer power and jamming geometry. Another approach is to cover all or part of the modulation range with a broadband jamming signal that is

received by the LPI radar receiver with adequate power to create adequate JSR in the "de-chirped" output.

Early research investigation of the anti-jamming aspect of linear FM pulse compression technique is provided in [3]. A mathematical model of a linear FM pulsed radar is constructed on the Signal Processing Workstation (SPW). The model generates a simulated chirp pulsed signal, which is added with selective interfering signals and evaluates the level of attenuation at the matched filter output. The experiment suggests that linear FM radar can recover useful echo signals under moderate white noise conditions. It also shows that the chirp radar, due to its high dependency on the frequency parameter for the matched filter implementation, is completely useless in differentiating a genuine chirp signal and a hostile jammer signal when the jammer produces signals that have a very similar frequency spectrum to the chirp signal [3].

Another document discussing detection and jamming of LPI radars has also provided some insight into FMCW jamming. It is suggested in [4] that false range targets may be displayed on an FMCW radar by slightly shifting the frequency of the return. The authors also suggest that velocity-gate pull-off (VGPO) can affect the signal processing in the radar. As far as noise jamming, narrow-band Doppler noise may also be quite effective since the signal-to-noise ratio (SNR) in the LPI receiver is already at quite a low value [4].

A brief discussion on FMCW jamming is seen in [5]. The author comments that FMCW can be easily overwhelmed by high-power pulse jammer. For that reason, FMCW radars are not generally used in military surveillance and weapons control systems.

With many existing discussions on FMCW jamming, this thesis project proposes a different research approach by looking into FMCW radar signal processing architecture in detail and seeks a possible EA solution. Experiments supporting the theoretical result are designed using both computer simulation and physical hardware. The MATLAB FMCW radar model is constructed to simulate the radar digital signal processing (DSP) response to different jamming waveforms. Hardware testing using LVRTS is also

conducted as an auxiliary measure of investigation. The thesis provides an in-depth investigation on FMCW jamming and can be used to verify the existing theories.

C. PRINCIPAL CONTRIBUTIONS

The research project provides an in-depth investigation on FMCW radar using all available approaches including theory, hardware experiment and computer simulation. The thesis discusses in detail FMCW radar DSP and its inherent capability of resisting interference. From the discussion of and references to other related work, an insight into effective jamming technique can be revealed.

The hardware experiment using LVRTS has shown the limits of the training tool for this project. Since LVRTS is marketed as an education system that is compacted with various radar capabilities, the circuitry does not provide the full functionality of each type of radar as it would have in a full-scaled radar system. For FMCW mode, the LVRTS only allows range measurement with no target Doppler preserved. Therefore, with the available equipment, only limited results can be drawn from the experiment, which is far from sufficient for conclusive results.

The MATLAB simulation model is constructed to compensate for the incapability of the hardware experiment. The radar model is constructed based on a homodyne FMCW radar signal processing procedure. The radar model can correctly evaluate the target range and velocity from the delay and Doppler shift of the received signal waveform. It is also capable of emulating the FMCW radar DSP response when the computer-generated jamming signals are applied. Also, the model is built in such way that most parameters have the freedom for adjustment for testing different scenarios.

From the results of all three approaches, the research concludes that from the DSP stand point, repeater jamming provides the most penetration to FMCW DSP, while requiring the least jamming power. Given the radar passband, pulse jamming can also be effective if sufficient pulse repetition frequency (PRF) is available. For noise jamming to be effective, the signal frequencies must be limited within the radar passband, as wideband noise jamming wastes much energy outside the radar band. From the EW standpoint, the effectiveness of jamming techniques highly depends on the information

available on the victim radar. For example, as studies suggest that repeater jamming is most effective against FMCW radar, in the real-world case when the emitter parameters are not available in the EA system library, repeater jamming may not work at all. In the worst case, in a noisy environment where the radar transmission band cannot be identified, barrage jamming may become the only EA option. In short, in the world of EW, there is no perfect jamming technique that can work in every scenario.

The thesis has provided a broad discussion and experiment results that may benefit many researchers in related fields. As the MATLAB simulation in this research is under a simple two-dimensional self-screen jamming scenario with no clutter involved, future modification of the program can be done for the study of angular deception by adding three-dimensional scan pattern to the model. With further development, complex FMCW jamming scenarios such as multi-target and battle-field meteorology can be simulated and studied.

D. THESIS OUTLINE

Chapter II provides an overview of the FMCW radar system including hardware architecture and signal processing principles. A homodyne FMCW radar system is used as an example of a typical FMCW architecture. The hardware components and their functionalities are explained individually in the order of the signal processing procedure. The principles discussed in this chapter are the prerequisites to the development of the MATLAB model to be used for jamming simulation.

In Chapter III, an attempt to test the jamming effect using a laboratory radar system is discussed. LVRTS is capable of target detection using a triangular-modulated FMCW waveform. The experiment deploys arbitrary waveform generators, which transmit jamming signals to the LVRTS receiver to emulate an EW jamming scenario. However, due to the internal circuitry design of LVRTS and limitations in jamming power, no decisive conclusion can be drawn.

Chapter IV presents a MATLAB model that emulates the functionality of the homodyne FMCW radar discussed in Chapter II. The model design and simulation algorithm are explained. An anti-ship capable missile (ASCM) scenario providing

simulation parameters is used to perform a signal-only simulation, in which the target echo is processed at the radar receiver model for target information (range and velocity).

Chapter V discusses the EA techniques against FMCW. The chapter begins with an investigation of the FMCW radar's inherent resistance to interference, which leads to a discussion on probable EA techniques in the succeeding section. The proposed jamming techniques, or waveforms, are modeled and tested for effectiveness using the FMCW MATLAB model.

Chapter VI elevates the discussion of FMCW jamming from simulation to the real-world EW application level. Given the proposed jamming techniques from Chapter V, the real-world implementation requirements, challenges and solutions are investigated. Also, the trends of future EA and EP measures are briefly discussed, before the research is concluded in Chapter VII.

II. FREQUENCY MODULATED CONTINUOUS WAVE RADAR

The high duty cycle feature of the continuous wave (CW) waveform spreads the transmitter power over time and reduces probability of interception. The most popular linear modulation waveform utilized is the triangular FMCW emitter, since it can measure the target's range and range rate [1].

This chapter explains the principle architecture and signal-processing algorithm of a homodyne FMCW radar to provide a general understanding of FMCW signal processing. Section A gives an overview of the signal processing procedure of a FMCW radar system, as well as a brief explanation of component functionalities. In Section B, mathematical expressions of triangular waveform are derived, as they are critical to the MATLAB simulation design to be discussed in the succeeding chapter. Sections C and D discuss the FMCW search mode and track mode signal processing. Finally, a laboratory FMCW radar system is presented as an example.

A. SINGLE ANTENNA FMCW RADAR ARCHITECTURE

The block diagram in Figure 1 illustrates the typical architecture of a single antenna FMCW radar. To transmit radar signals and receive target echo simultaneously through a single antenna, a circulator is used to provide individual channels for both signals. A reflective power canceller (RPC) nullifies the transmitter leakage at the receiver to achieve high insolation, which avoids degrading sensitivity [6]. The mixer takes a portion of the transmitting signal and uses it as the reference signal that correlates the received echo signal. The resultant output is what is called a *beat signal* whose frequency is proportional to the propagation time of the radar signal. This mixing process also down-converts the radio frequency (RF) signal to an intermediate frequency (IF) signal. IF signal is preferred in signal processing because components that operate at high frequency are less stable and more expensive.

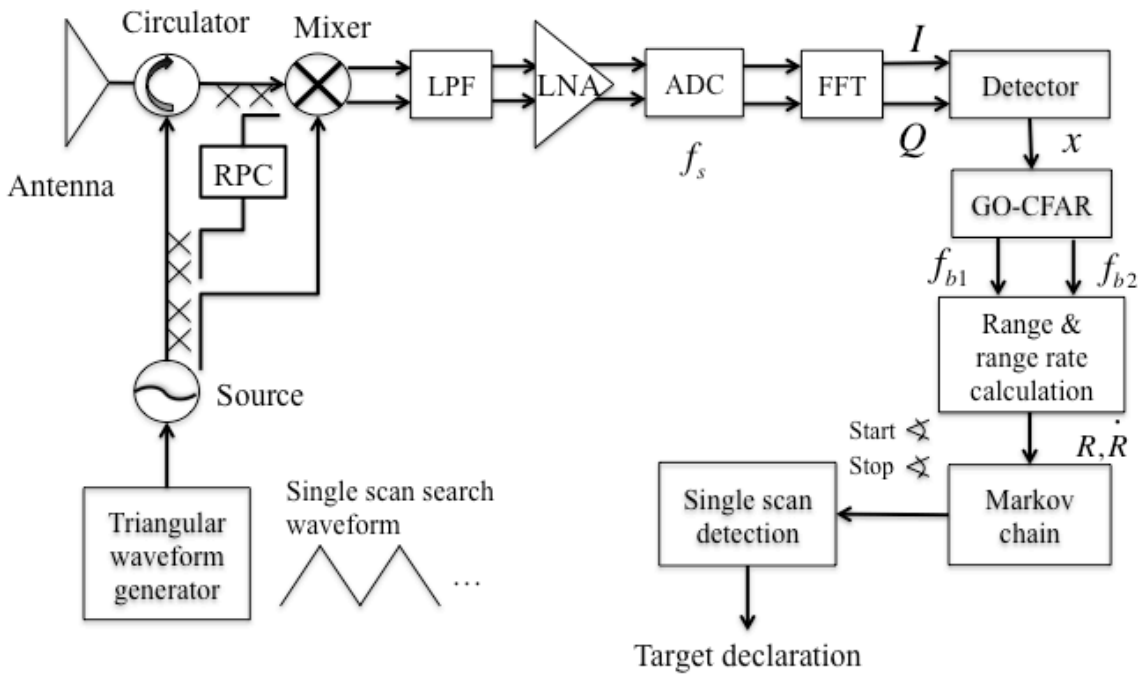

Figure 1. Block Diagram of a homodyne triangular FMCW radar (after [1]).

A low-pass filter is located at the mixer output to filter out unwanted signal noise. The filter cutoff frequency is set at the maximum beat frequency corresponding to the maximum detectable range for which the radar is designed. As the beat frequency is much lower than the echo signal frequency, only a fraction of received noise can reach the low noise amplifier (LNA). This limits the amount of noise being amplified, which can cause unwanted clutter in the signal spectrum and affect detection efficiency [1].

A complex analog-to-digital converter (ADC/CADC) digitizes the complex analog signal. The complex ADC outputs (I/Q channel) are then evaluated in the frequency domain using an FFT computation. An envelope approximation detector measures the magnitude of both in-phase and quadrature signals and computes the overall signal spectral magnitude approximated by

$$x = a\max\{|I|,|Q|\} + b\min\{|I|,|Q|\} \tag{2.1}$$

where a and b are the simple multiplying coefficients [7]. An envelope approximation detector is useful because a radar computer can perform the calculations easier and faster

than the $\sqrt{I^2+Q^2}$ approach. However, different choices of a and b result in a different error. An in-depth investigation of an envelope approximation detector can be found in [7].

The Greatest of Constant False Alarm Rate detector (GO-CFAR) searches for target signals in the magnitude spectrum. Figure 2 illustrates an *n*-cell GO-CFAR structure. The detector can be thought of as a sliding window, moving from low to high along the frequency spectrum axis, with a test cell in the middle and n numbers of reference cells on the each side. The signal magnitude under the test cell is measured and compared with the threshold voltage V_T . When the test cell voltage is above the threshold limit, the detector considers there is a target within that bin. On the other hand, if the test cell voltage is less than the threshold voltage, no target is detected at that test cell.

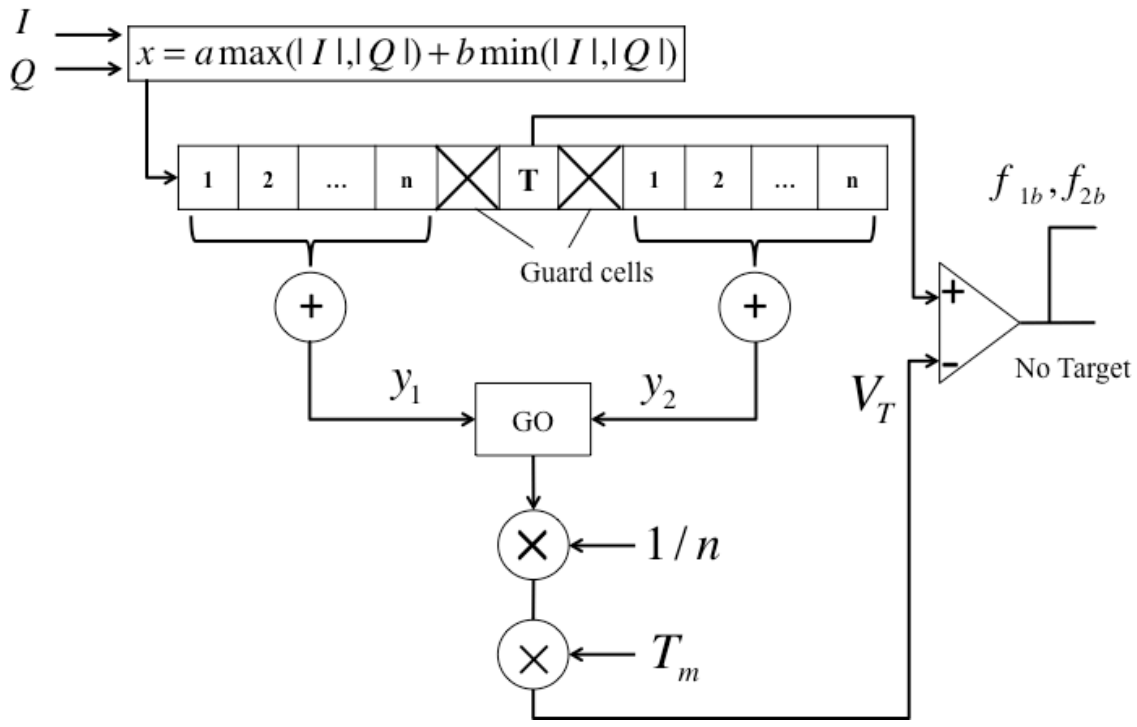

Figure 2. Envelope approximation detection GO-CFAR processor (after [1]).

The threshold voltage depends on the average signal voltage within the reference cells on each side of the test cell. The summations of signal voltages at the reference cells on each side, y_1 and y_2, are compared in magnitude. The voltage with greater value is then divided by n for the average signal magnitude in each reference cell, before multiplying by a threshold multiplier T_m, and then becomes the threshold voltage V_T. The value of the threshold multiplier depends on the minimum allowable probability of false alarm (PFA) of the GO-CFAR detector.

Due to the possible power leakage in magnitude spectrum, often a few extra cells (known as guard cells) are added on each side of the test cell as isolation [8]. This technique is used in the MATLAB model, which will be discussed in Chapter IV.

The output of GO-CFAR is the filter where targets are detected. Targets are declared for both up-chirp and down-chirp (beat frequency f_{1b} and f_{2b} respectively.) of the triangular modulation. The actual target position and velocity can be calculated with the sum and difference between f_{1b} and f_{2b}. Section B discusses mathematical expression of FMCW triangular modulation, as well as target range and velocity calculation in detail.

B. FMCW TRIANGULAR WAVEFORM DESIGN

This section explains the FMCW triangular waveform architecture and how parameters are determined. The principles also apply to the parameter design used in the simulation, which will be discussed in the next chapter.

1. Transmitted Signal

Since a FMCW waveform is deterministic, it can be described entirely in a mathematical manner. The frequency of the first section (up-chirp) of the transmitted waveform is expressed as [1]:

$$f_1(t) = f_c - \frac{\Delta F}{2} + \frac{\Delta F}{t_m} t \tag{2.2}$$

where f_c is the signal carrier frequency, ΔF is the modulation bandwidth, and t_m is the modulation period. Figure 3 illustrates the triangular waveform modulation and resultant beat frequency.

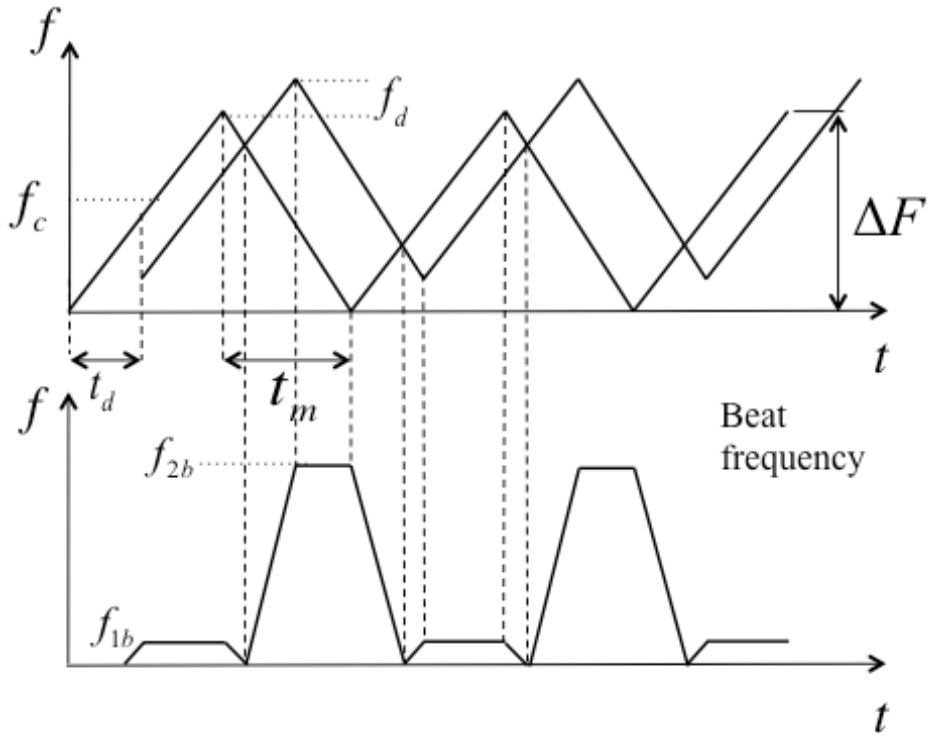

Figure 3. Linear frequency modulated triangular waveform and the Doppler shifted received signal (after [1]).

The phase of the transmitter RF signal is [1]

$$\Phi_1(t) = 2\pi \int_0^t f_1(x)dx \tag{2.3}$$

From (2.2) and (2.3)

$$\Phi_1(t) = 2\pi \left[\left(f_c - \frac{\Delta F}{2} \right) t + \frac{\Delta F}{2t_m} t^2 + \frac{2V}{\lambda} t \right] \tag{2.4}$$

The complex form of the transmitted signal waveform is

$$S_{t1}(t) = e^{j\Phi_1(t)} \tag{2.5}$$

Therefore,

$$S_{t1}(t) = \exp\left\{ j2\pi \left[\left(f_c - \frac{\Delta F}{2} \right) t + \frac{\Delta F}{2t_m} t^2 \right] \right\} \tag{2.6}$$

For the second section (down-chirp) triangular waveform:

$$f_{t2}(t) = f_c + \frac{\Delta F}{2} - \frac{\Delta F}{t_m} t \tag{2.7}$$

The same derivation applies to the second section. The equation is therefore

$$S_{t2}(t) = \exp\left\{ j2\pi \left[\left(f_c + \frac{\Delta F}{2} \right) t - \frac{\Delta F}{2t_m} t^2 \right] \right\} \tag{2.8}$$

2. Received Signal

The received signal can be expressed as the transmitted waveform with a round-trip time delay t_d. In the case of a moving target, the Doppler frequency shift must also be included in the equation. The Doppler shift of a target with relative velocity V is

$$f_{doppler} = \frac{2V}{\lambda_c} \tag{2.9}$$

Therefore, the received signal frequency becomes

$$f_{r1}(t) = f_c - \frac{\Delta F}{2} + \frac{\Delta F}{t_m}(t - t_d) + \frac{2V}{\lambda_c} \tag{2.10}$$

$$f_{r2}(t) = f_c + \frac{\Delta F}{2} - \frac{\Delta F}{t_m}(t - t_d) + \frac{2V}{\lambda_c} \tag{2.11}$$

where t_d is the propagation delay of the received waveform, V is the relative target velocity and λ_c is the wavelength of the carrier frequency.

Note that λ_c is an approximation of the instantaneous wavelength at time t, as the actual wavelength varies with time. The approximation is appropriate as the modulation bandwidth is small relative to the carrier frequency.

$$\Phi_{r1}(t) = 2\pi\left[\left(f_c - \frac{\Delta F}{2}\right)(t-t_d) + \frac{\Delta F}{2\cdot t_m}(t-t_d)^2 + \frac{2V}{\lambda}(t-t_d)\right] \tag{2.12}$$

Same as (2.6), the returned signal from the point target can be presented as

$$S_{r1}(t) = \exp\left\{j2\pi\left[\left(f_c - \frac{\Delta F}{2}\right)\cdot(t-t_d) + \frac{\Delta F}{2\cdot t_m}(t-t_d)^2 + \frac{2V}{\lambda}(t-t_d)\right]\right\} \tag{2.13}$$

Similarly, for the second section

$$\Phi_{r2}(t) = 2\pi\left[\left(f_c + \frac{\Delta F}{2}\right)(t-t_d) - \frac{\Delta F}{2\cdot t_m}(t-t_d)^2 + \frac{2V}{\lambda}(t-t_d)\right] \tag{2.14}$$

$$S_{r2}(t) = \exp\left\{j2\pi\left[\left(f_c + \frac{\Delta F}{2}\right)\cdot(t-t_d) - \frac{\Delta F}{2\cdot t_m}(t-t_d)^2 + \frac{2V}{\lambda}(t-t_d)\right]\right\} \tag{2.15}$$

C. SEARCH MODE SIGNAL PROCESSING

The capability of target detection is closely related to the parameter design of the modulation waveform. The key parameters of FMCW modulation are the modulation bandwidth and modulation period. Modulation bandwidth is determined depending on the desired range resolution of the radar.

$$\Delta F = \frac{c}{2\Delta R} \tag{2.16}$$

where ΔR is the desired range resolution; ΔF is the modulation bandwidth; $c \approx 3\times 10^8$ m/s is the speed of light.

An imaging radar system requires wide modulation bandwidth in order to obtain high range resolution, which allows the resultant Range-Doppler image to present the structure features of the target. On the other hand, for search radar, range resolution needs to be greater than the target length in order to avoid the returned signal being spread across multiple range bins in the spectrum and to avoid an increase in the PFA.

The modulation period of the transmitted waveform is critical for moving target acquisition. From the radar perspective, maintaining a moving target in the same range bin throughout a modulation period is desired [1]. Otherwise the target smears in the

spectrum and causes detection difficulties. To detect a target of maximum velocity $V_{\max}$, the required modulation period t_m is

$$t_m < \frac{\Delta R}{V_{\max}} \tag{2.17}$$

Another condition is that t_m should be several times the maximum round-trip delay t_d. This condition minimizes the loss in effective transmit bandwidth and power and also provides a high velocity resolution [1].

Due to the time differences between the transmitted and received waveform, only part of the modulation period is utilized in search mode signal processing. Recall from Figure 3 that for each up-chirp or down-chirp section, only within the time interval where both transmitted and received waveform have identical chirp rate can the beat frequency be evaluated correctly at the FFT stage. Therefore, the time interval of interest within one modulation period is the difference between t_m and t_d. However, since a target echo delay varies depending on the target position, the coherent processing interval of a radar system is determined based on the maximum detectable range for which the system is designed. The coherent processing interval of a radar system with t_m modulation period is calculated as

$$t_o = t_m - t_{d\max} \tag{2.18}$$

where $t_{d\max}$ is the maximum echo delay expected by the radar. This allows the echo signal to be processed correctly for any in-bound target while keeping the coherent processing interval constant, which greatly reduces hardware complexity, as shown in Figure 4.

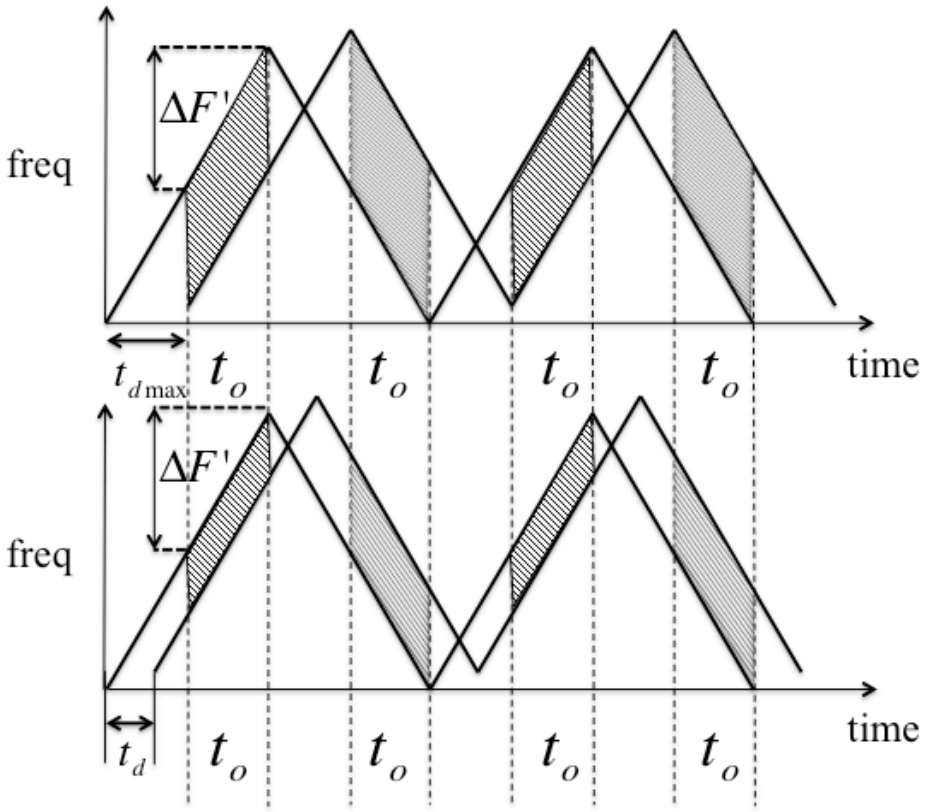

Figure 4. Coherent processing interval at maximum detectable range (above) and in-ranges (below).

The effective bandwidth within the coherent processing interval is then

$$\Delta F' = \Delta F(\frac{t_o}{t_m}) \text{ Hz} \tag{2.19}$$

The beat frequency for the 1st and 2nd section is then

$$f'_{1b} = \frac{2R\Delta F'}{ct_o} - \frac{2V}{\lambda} \tag{2.20}$$

and

$$f'_{2b} = \frac{2R\Delta F'}{ct_o} + \frac{2V}{\lambda} \tag{2.21}$$

with both beat frequencies calculated, the target range can be computed as

$$R = \frac{ct_o}{4\Delta F'}(f'_{1b} + f'_{2b}) \text{ m} \tag{2.22}$$

and the target's range rate is calculated as

$$\dot{R} = \frac{\lambda}{4}(f'_{2b} - f'_{1b}) \text{ m/s} \tag{2.23}$$

Note that Equations (2.20) and (2.21) are provided only for the completeness of the theory. In the MATLAB simulation to be discussed, the beat frequencies are evaluated by correlating the transmitted and received signals, as they would be in an actual FMCW system.

D. TRACK MODE SIGNAL PROCESSING

Once a target is detected in the search mode, the FMCW tracking mode is needed to lock-on and monitor the target. There are two different approaches to track the target position.

The first approach is to keep the target beat frequency constant by varying the transmitter bandwidth [1]. Recall that in the search mode signal processing, the detected target range is computed from the measured beat frequency f_{1b} and f_{2b} (2.22). A target detected at f_{1b} and f_{2b} will show up in filter f_b in the track mode signal processing.

$$f_b = \frac{f_{b1} + f_{b2}}{2} \tag{2.24}$$

Using this relationship, (2.19) can therefore be arranged as

$$\Delta F' = \frac{cf_b t_o}{2R} \tag{2.25}$$

This tracking approach requires the detected target beat frequency to remain in filter f_b. With $cf_b t_o$ being a constant, the effective bandwidth needed becomes larger as the range to target gets smaller. This algorithm requires constant adjustments of the transmitting signal bandwidth based on the target range calculated in each sweep. The major advantage of this approach is that since the target beat frequency is a constant value, a

narrow-band pass filter centering this frequency can be designed to filter out noise and increase SNR.

The second approach is to maintain the transmitting bandwidth and allow the beat frequency to vary. The target's position can be followed in signal processing by monitoring the position of the FFT peak detector output. The advantage of this method is that the receiver LPF used in the search mode can also be used for the track processing [1].

E. SUMMARY

This chapter provides the essential theory of FMCW signal processing techniques. Both homodyne FMCW radar signal processing algorithm and triangular modulation waveform design are discussed. However, for the scope of this project, post-detection signal processing is left out for future investigation.

The next chapter provides a discussion on the attempt to investigate FMCW jamming using a laboratory radar system. An experiment is designed to conduct EA by having an arbitrary waveform generator and Radar Jamming Pod Trainer generate interfering signal into the radar receiver and observe for effectiveness. However, due to the limited capability of the hardware, only limited results can be obtained. The chapter starts with an introduction to LVRTS, followed by a discussion of experiment design and problems encountered. The experiment is therefore adjusted to adapt to the hardware limitations. The result of the compromised test is also discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FMCW JAMMING WITH LAB-VOLT RADAR TRAINING SYSTEM

LVRTS is a laboratory radar system that is compatible with several radar configurations, including FMCW. The compact and low-power characteristics of LVRTS allow it to be operated safely and make it prime for a laboratory environment. An investigation on FMCW jamming by applying jamming waveforms to the LVRTS was attempted. However, due to the constraint of the hardware, no significant result was found in this experiment.

This chapter briefly introduces the Lab-Volt system, jamming test method and results. Also, the constraints of the system are discussed.

A. INTRODUCTION TO LAB-VOLT RADAR TRAINING SYSTEM

LVRTS is a laboratory radar system designed to demonstrate the principles and scenarios of electronic warfare for training purposes. It is highly configurable for different radar searching and tracking techniques, target parameters and several EA techniques. The radar system can be configured as pulse Doppler, CW or FMCW radars depending on the training objectives. The Moving Target Indication (MTI) processor and Moving Target Detection (MTD) processor are also included in this equipment. The Target Positioning System can provide a moving target of interchangeable size and shape for target-acquiring experiments. The radar jamming pod trainer is capable of performing direct or modulated noise jamming as well as repeater jamming. Other sub-systems featuring synthetic-aperture radar (SAR), inverse synthetic-aperture radar (ISAR), RCS measurement and phase array technology are also available.

Despite the wide-range functionality provided by LVRTS, the system does not represent a full-scale radar system with any of its configurations, as it is specifically designed for the experimental courses and procedures provided by the manufacturer. Although CW and FMCW modes are available for the LVRTS transmitter, most signal processing and EW scenario provided by the system are built under pulse Doppler radar

mode. In the manufacturer course design, CW and FMCW mode are simply used to demonstrate the principle of these types of radars.

The FMCW mode of LVRTS has limited capabilities. It is limited to triangular waveform modulation at a fixed carrier frequency of 9.4 GHz, with a slightly adjustable modulation period and bandwidth. A block-diagram of LVRTS FMCW configuration is shown in Figure 5. The FMCW output of the system is the beat signal, which can be observed on an oscilloscope. When the FMCW output is connected to a frequency counter, the beat frequency can be measured and the target range can be calculated by hand. As this research is interested in investigating how different jamming techniques can affect FMCW in detecting target range and velocity, a project to build a MATLAB program capable of processing the FMCW output that can evaluate both target range and velocity is proposed. With the ability to correctly process the FMCW output signal, the system can be tested for its response to EA attack by applying different jamming waveforms using an arbitrary waveform generator.

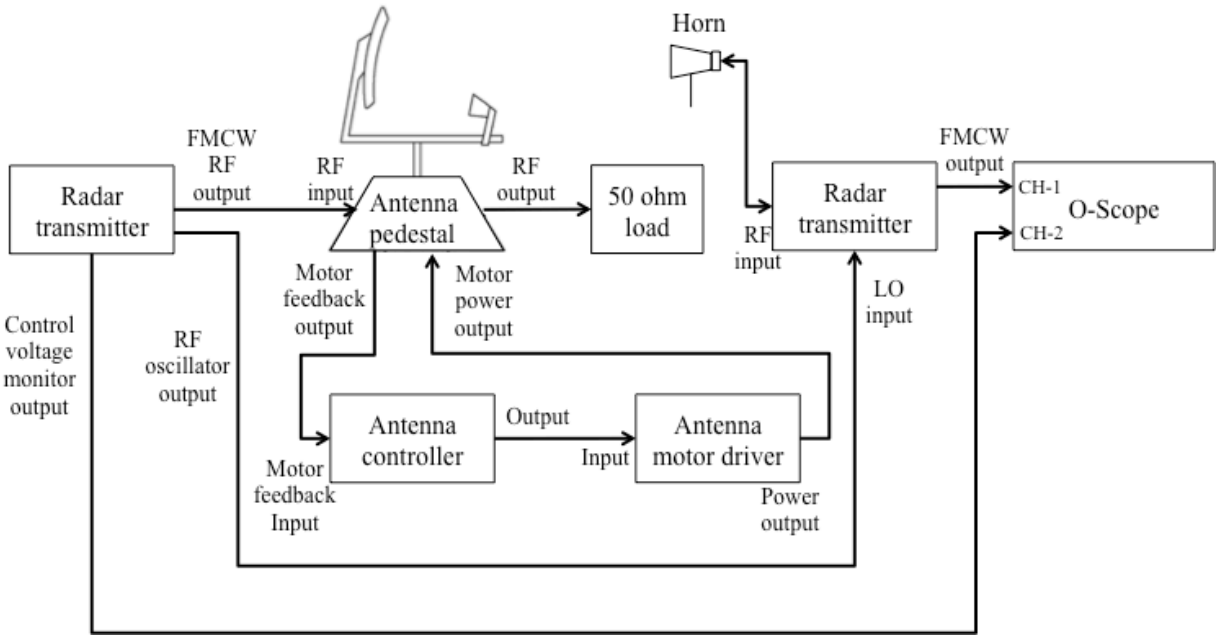

Figure 5. Block diagram of FMCW radar configuration (after [9]).

B. ATTEMPTED LVRTS EXPERIMENT DESIGN

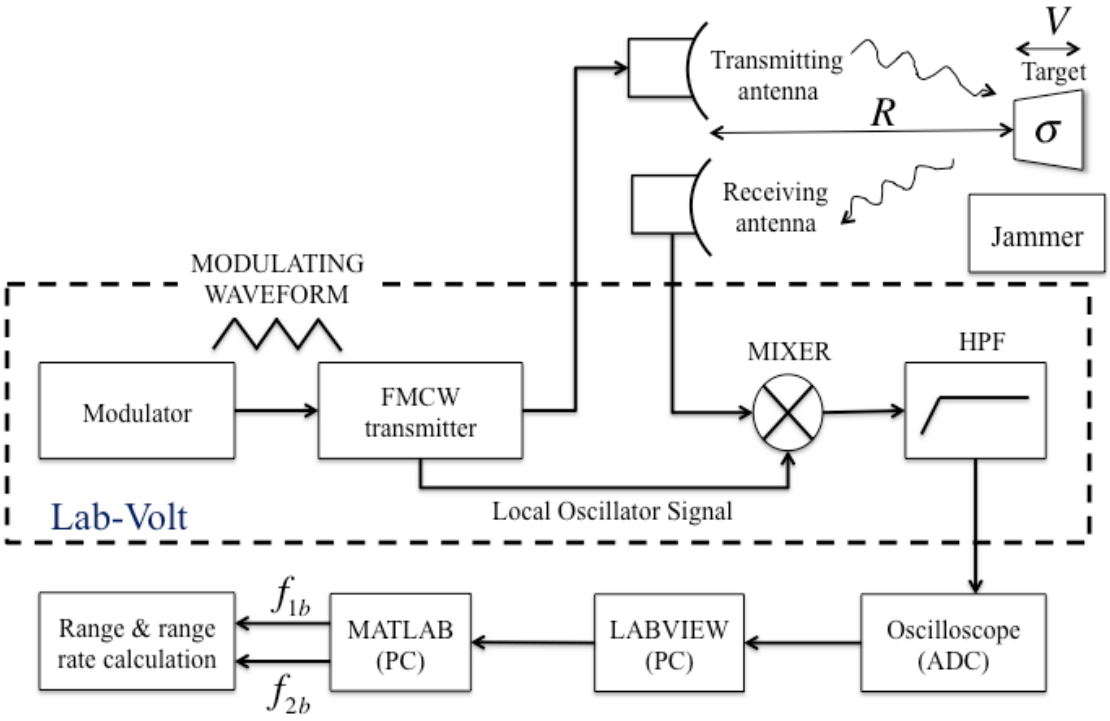

Figure 6. Attempted FMCW jamming test using LVRTS.

The FMCW jamming test design is shown in Figure 6. The design of the experiment is first to put a metal plate target in motion along the radar line of sight using Target Positioning table, as shown in Figure 7. The LVRTS transmits triangular-modulated FMCW waveform to illuminate the target and receiver target echo at the receiving antenna. The FMCW output signal is then digitized to an ADC and quantized at the LABVIEW program. The output of LABVIEW is an Excel array containing the magnitude samples of the signal. This array is then put into MATLAB to evaluate the beat frequency and calculate for target range and range rate. For EA testing, one or more arbitrary waveform generators can be implemented to perform several jamming techniques that interfere with the received signal. The jamming effect can be evaluated by observing the change in target range and velocity computed in MATLAB.

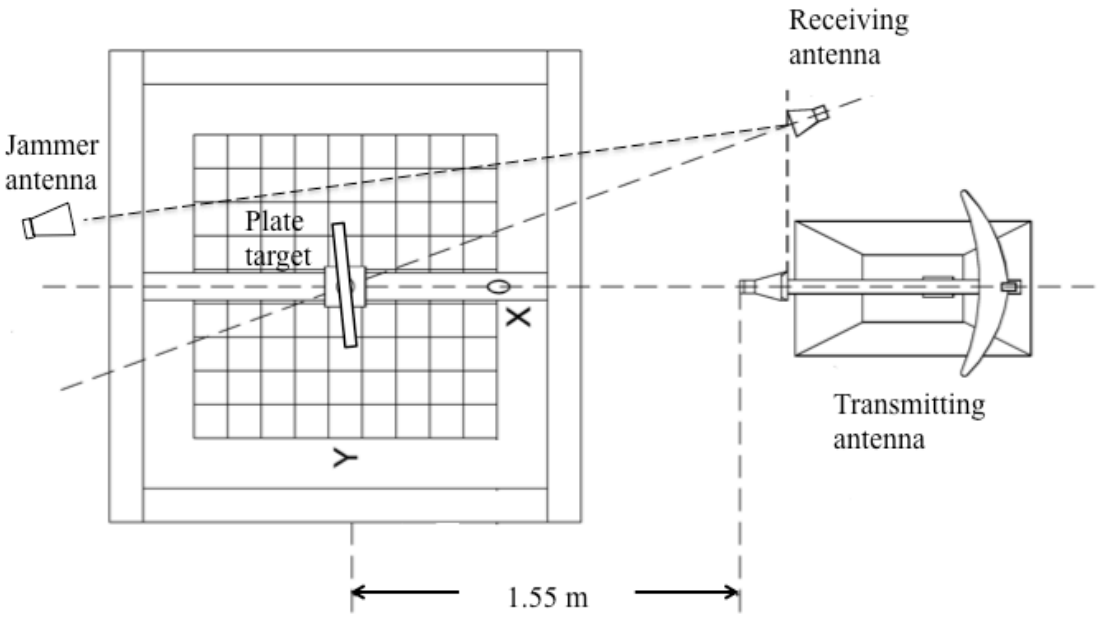

Figure 7. LVRTS antennas and plate target (after [9]).

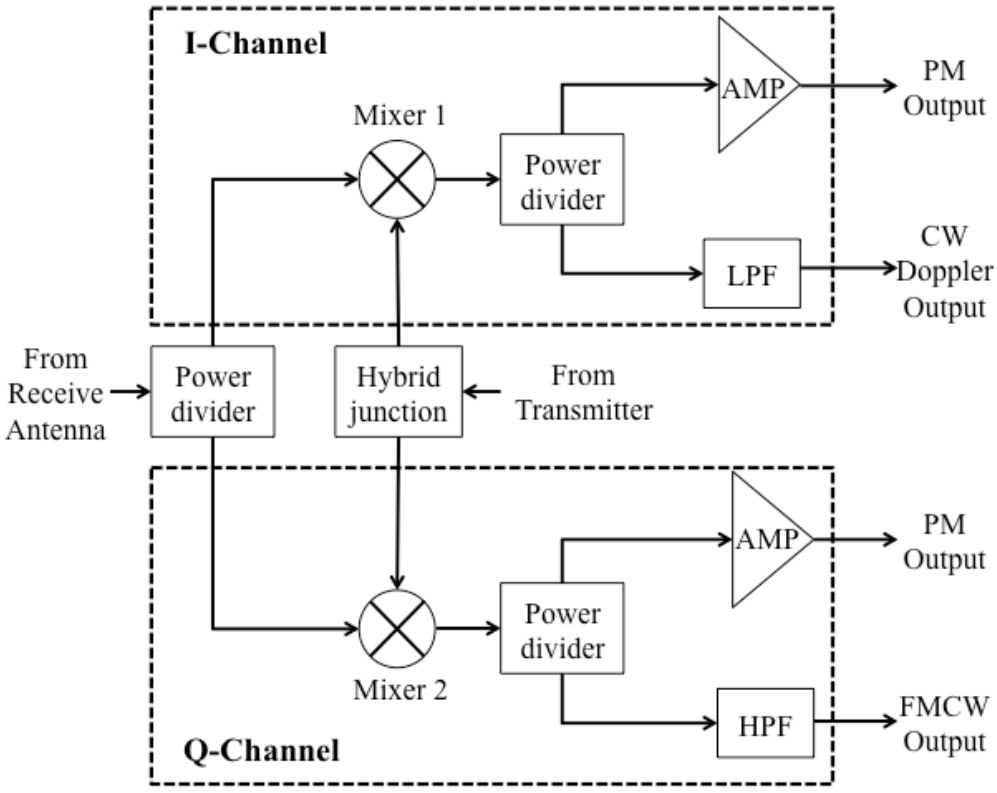

Figure 8. LVRTS receiver module block diagram (after [10]).

The experiment was, however, unsuccessful as the LVRTS signal processing does not preserve the Doppler information of the returned signal. As shown in the receiver block-diagram depicted in Figure 8, the received signal is filtered by a 1 kHz high-pass filter (HPF) prior to the FMCW output. This HPF is designed for the purpose of reducing possible clutter resulted from close object in a laboratory environment (i.e., the front edge of the target table) and ensures accurate range measurement. However, this filtering also erases the Doppler frequency embedded in the signal, as Doppler measurement is not intended in LVRTS design.

C. JAMMING TEST USING ARBITRARY WAVEFORM GENERATOR

Given that the LVRTS is only capable of range measurement, a compromised test is run by simply observing the change in beat frequency, while applying jamming signals to the radar receiver. This extended test deploys signal generators and matched horn antennas as adversary jammers, which are attempting to corrupt the signal going into the LVRTS receiver, hence corrupting the interpreted beat frequency.

The LVRTS is set to FMCW mode where $f_c = 9.4$ GHz, $f_m =$ 1 kHz and $\Delta F =$ 1 GHz. The radar illuminates a plate target 1.55m away, located at the center of the target table, and receives the reflected waveform. Under no jamming circumstances is the beat frequency shown on the frequency counter on the order of 40 kHz. The experiment set up is as shown in Figure 7. Note that the jammer horn antennas are located at approximately 15 degrees from the peak of receiving antenna main beam. Jamming techniques are tested for the target range 1.1m, 1.55m and 2m away from the radar pedestal.

First, a tone jamming signal set at radar center frequency 9.4 GHz is injected into the radar. To avoid excessive jamming power damaging the LVRTS receiver circuits, the power level is limited to 0 dBm. When the plate target is 1.1 meter from the radar antenna, almost no jamming effect is observed. At 1.55m, the jamming effect is also minimal. When target is positioned at 2m away from the radar antenna, the extended range increases the JSR, thus a slight increment of beat frequency can be observed from the frequency counter. The tone jamming result is summarized in Table 1. Note that since

the beat frequency measured by the frequency counter fluctuates, the test for each range is run five times. The result is an averaged value from all five trials.

Table 1. LVRTS tone jamming result.

Target Range (m)	Avg. Beat Frequency	Avg. Beat Frequency (Hz)	Avg. Error (Hz)
1.10	34,816	34,817	2.6
1.55	39,942	39,955	6.6
2.00	47,288	47,438	147.8

A triangular FMCW signal is also tested using the same procedure. For the best jamming result, the jamming signal is modulated according to the radar modulation parameter, with center frequency of 9.4 GHz and 1 ms modulation period. However, due to equipment capability, only 10 MHz modulation bandwidth is available, whereas 1 GHz is desired. The test result is shown in Table 2. Although the modulation parameter is not ideal, the triangular FMCW jamming has a more significant effect on the radar than does tone jamming.

Table 2. LVRTS Triangular FMCW jamming result.

Target Range (m)	Avg. Beat Frequency	Avg. Beat Frequency (Hz)	Avg. Error (Hz)
1.10	34,816	34,867	51
1.55	39,942	40,049	113.6
2.00	47,288	47,514	206.6

To compare the differences between modulation waveforms, a sinusoidal FMCW signal is also tested. The modulation parameter is identical to the previous test except the modulation waveform. From Table 3, it can be seen that sinusoidal FMCW jamming also has obvious effect to the radar beat frequency.

Table 3. LVRTS Sinusoidal FMCW jamming result.

Target Range (m)	Avg. Beat Frequency	Avg. Beat Frequency (Hz)	Avg. Error (Hz)
1.10	34,816	34,869	52.6
1.55	39,942	40,031	84.2
2.00	47,288	47,483	184.8

During the pulse jamming test, the radar is injected with a pulse jamming signals with pulsewidth of 10 μs, carrier frequencies of 9.4 GHz and PRF of 10 kHz. As the signal generator power is limited to 0 dBm, no jamming effect is observed at all ranges.

The Lab-Volt Radar Jamming Pod Trainer provides the capability of generating a band-limited random noise jamming signal that can be used for the experiment. The noise is centered at 9 GHz with 1 GHz bandwidth. The band-limited random noise has relative strong effect to the radar beat frequency when the target is placed 2m from the radar, as shown in Table 4.

Table 4. LVRTS random noise jamming result.

Target Range (m)	Avg. Beat Frequency	Avg. Beat Frequency (Hz)	Avg. Error (Hz)
1.10	34,816	34,896	78
1.55	39,942	40,019	80.2
2.00	47,288	47,512	255.2

The effectiveness of test jamming waveforms is compared in Table 5. Band-limited random noise has induced the most beat frequency error at radar-to-target range of 1.1m and 2m, whereas the triangular FMCW has strongest effect on the 1.55-meter trial. Sinusoidal FMCW is slightly less effective than triangular FMCW, with tone jamming being the least effective jamming waveform.

Table 5. Beat frequency error induced by different jamming waveforms (Hz).

Range (m)	Tone jamming	Triangular FMCW	Sinusoidal FMCW	Random Noise
1.10	2.6	51	52.6	78
1.55	6.6	113.6	84.2	80.2
2.00	147.8	206.6	184.8	255.2

However, the result from this experiment can only provide limited information and is insufficient for drawing a conclusive result. From Table 5, it can be seen that the results have obvious inconsistency, as the random noise jamming being the most effective at 1.10-meter trial and 2-meter trial but next to the least effective at 1.55-meter trial. Also the errors induced by each jamming waveform are too little to make a fair comparison. For random noise, which has induced the most beat frequency error (255.2 Hz), the corresponding range error is less than 2 cm. Therefore, the small amount of difference between jamming results does not confirm that one jamming technique is more effective than the others. The test results are plotted in Figure 9. Notice that the results from different jamming waveforms are almost indistinguishable for each range.

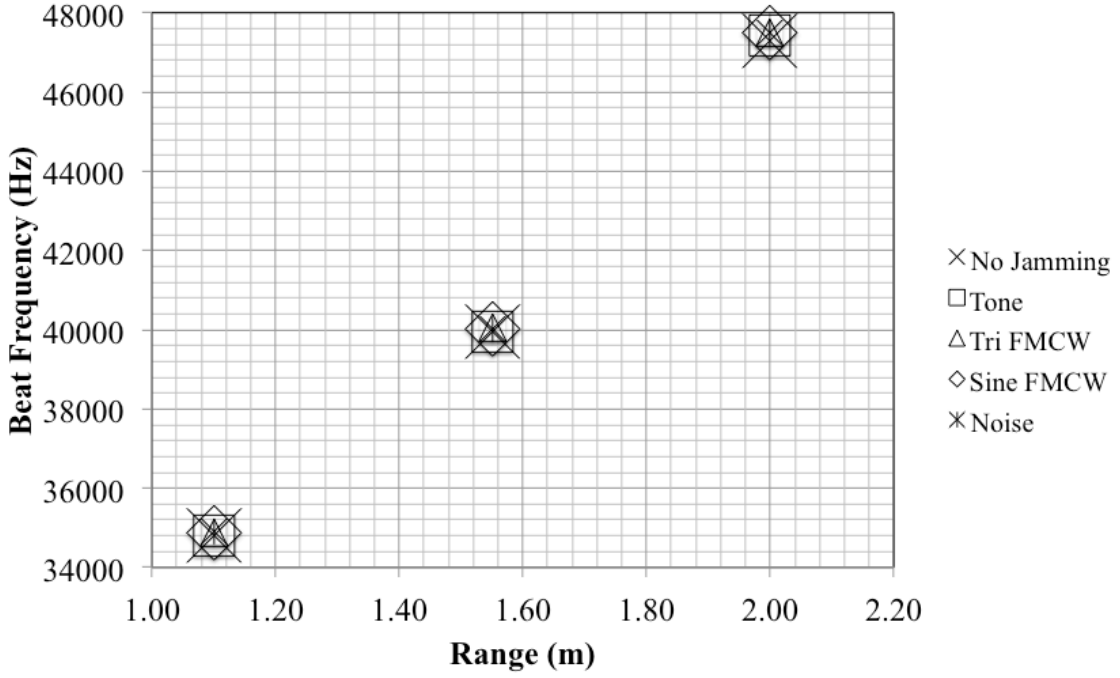

Figure 9. LVRTS jamming test result.

Hardware constraints are also a major factor that influences the test result. To prevent high jamming power from damaging the radar receiver circuitry, the jamming power is limited to 0 dBm. The power constraint has limited the variance of the jamming result, making it difficult to compare jamming effectiveness between different waveforms. Furthermore, the power constraint has paralyzed the pulse jamming signal, which requires high peak power to be effective, especially against FMCW radar. Another hardware problem is that the signal generator is not capable of generating a FMCW jamming waveform having the same chirp rate as the radar signal waveform. Theoretically, a jamming waveform that has the same modulation parameter as the victim radar can be very effective in FMCW jamming [1].

D. SUMMARY

Due to the circuitry design of the receiver, the attempt to investigate the effectiveness of EA interfering with target range and range rate using LVRTS was unsuccessful. By simply observing the beat frequency variance under the jamming condition, few conclusions can be drawn. Testing with high jamming power may provide more constructive results, but the potential for damaging the LVRTS circuit always exists. It can be concluded that LVRTS does not provide the precision and stability required for an in-depth jamming experiment.

With the hardware test failing to provide decisive results, the research has turned to a computer-simulation project using MATLAB, which provides enhanced accuracy and choices of jamming techniques. The next chapter introduces the design of a radar model that is capable of emulating a FMCW radar DSP behavior. A simulation result based on an ASCM scenario is also presented.

THIS PAGE INTENTIONALLY LEFT BLANK

.

IV. SIMULATION DESIGN

This chapter introduces the design of the MATLAB model used for the FMCW jamming simulation. The simulation scenario is based on an ASCM scene with the missile as the FMCW emitter and the ship as the jammer. The radar model is constructed based on the principle and architecture of FMCW radar signal processing discussed in Chapter II. This chapter also provides the simulation results without the jamming signal applied. The jamming simulation is discussed separately in Chapter V.

A. ASCM SCENARIO

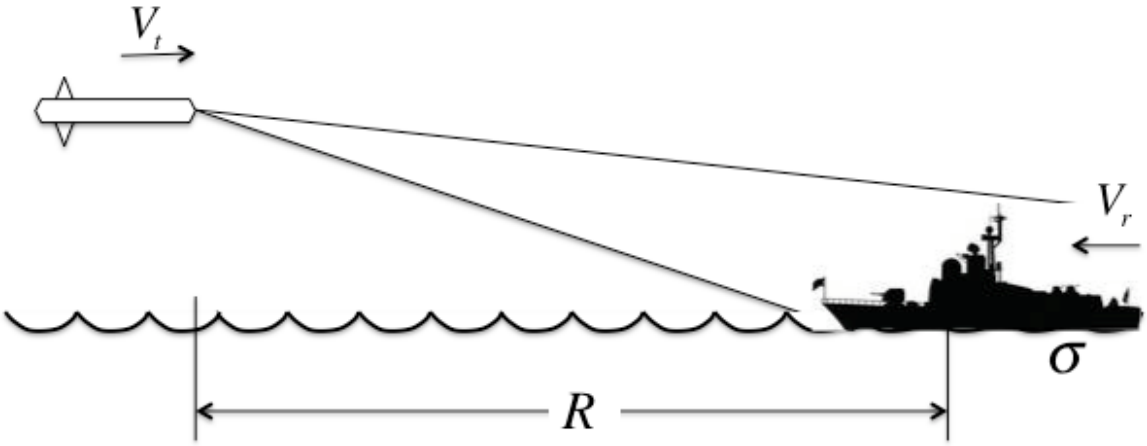

Figure 10. ASCM LPI emitter-ship scenario.

In the simulation scenario, an antiship missile is launched to attack a low radar cross-section（RCS) warship as shown in Figure 10. The missile, traveling at $V_t = 300$ m/s, utilizes an FMCW seeker with triangular modulation. The range to the target is 21 km when the emitter starts transmitting. The warship has a RCS of $500\,\mathrm{m}^2$ and is moving at a speed of $V_r = 0$ m/s. That is, the ship can be assumed to be stationary with respect to the missile, thus the missile-to-target closing velocity V is 300 m/s. With early intelligence, the warship is able to locate the incoming missile on the radar screen in the early stages. An onboard jammer is used to perform EA against the missile's seeker. The missile emitter parameter design is listed in Table 6.

Table 6. MATLAB Emitter Parameter Design.

Carrier frequency	f_c	4 GHz
Modulation period	t_m	1.0 ms
Coherent processing interval	t_o	800 μs
Modulation bandwidth	ΔF	15 MHz
Effective modulation bandwidth	$\Delta F'$	12 MHz
Range resolution	ΔR	10.0 m
Effective range resolution	$\Delta R'$	12.3 m
FFT size	$NFFT$	8,192
Average transmitter power	P_t	Adaptive
ADC sampling speed	f_s	6.02 MHz
Detection signal-to-noise ratio	SNR_{Ro}	20 dB
Receiver Noise factor	F_R	10
Filter width	Δf	735 Hz
System losses	L	10
Antenna gain	G	810
Number of modulation periods	N	10

B. FMCW RADAR MODEL

The Radar Model is built following the same DSP procedure discussed in Chapter II. Individual radar components are emulated in separate coding sections. Figure 11 is the first level MATLAB model block diagram. Note that circulator and low noise amplifier are omitted as they are not necessary in the computer simulation. The following sections discuss the design and algorithm of each component individually.

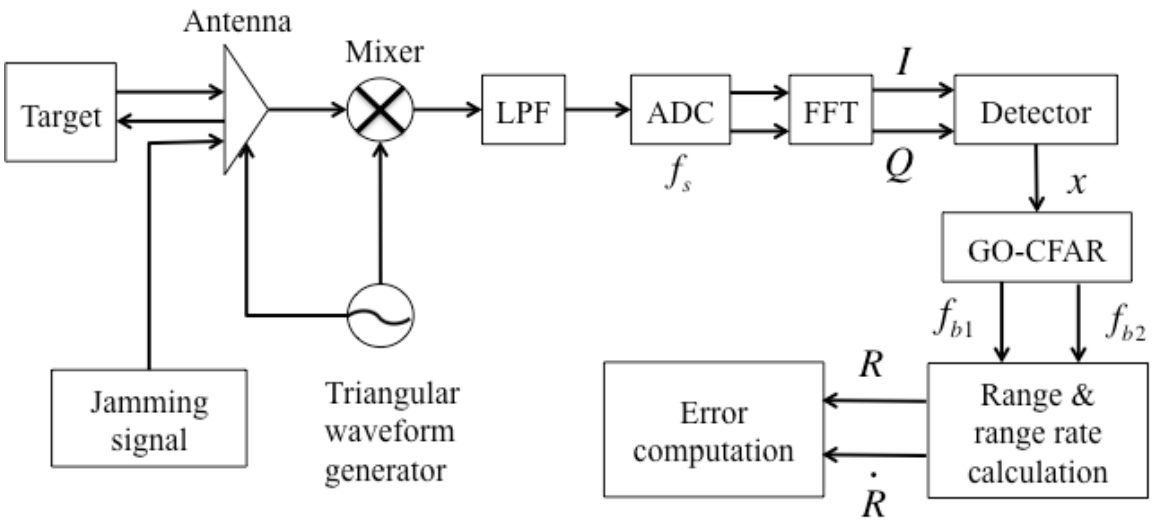

Figure 11. First level MATLAB FMCW radar jamming model block diagram.

1. Transmitter Model

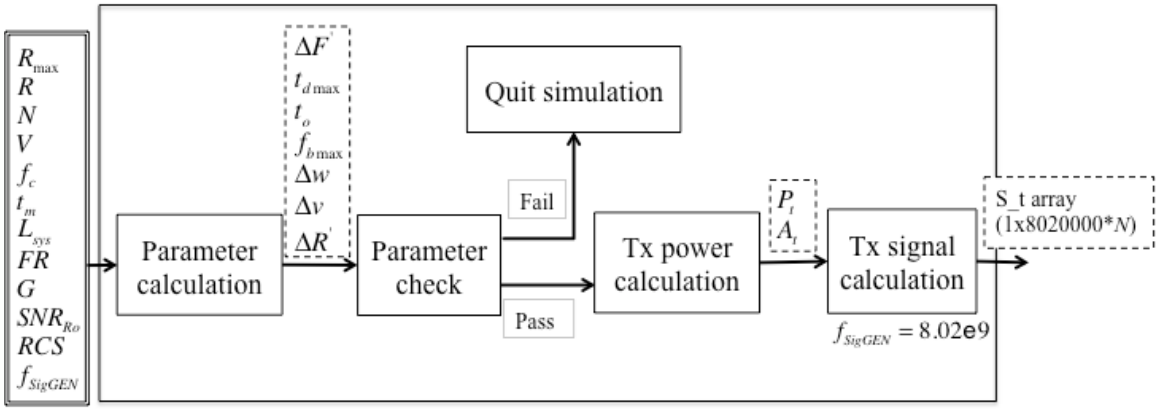

Figure 12. Transmitter MATLAB model block diagram.

In the transmitter model shown in Figure 12, the input target range and velocity are first evaluated with (2.17) to determine whether the target could be correctly detected with the current system parameter design. Since the model involves array operations, which require the array index to be integers, this stage also evaluates if all input variables can be correctly processed at a later stage. If the parameter-check fails, the simulation is interrupted; otherwise it proceeds to compute transmitting signal.

To determine the amplitude of the transmitted waveform, A_t, the required transmitter average power must be calculated in the first place. Due to the implementation of the power managing system, the value of transmitted power is adaptive to keep a constant SNR as the target range decreases.

The average power is calculated as [1]

$$P_t = \frac{(4\pi)^3 kT_o F_R L \Delta f}{G^2 \lambda} \left(\frac{R^4 SNR_{Ro}}{\sigma} \right) \tag{4.1}$$

where F_R is the receiver noise factor. $kT_o = 4.0 \times 10^{-21}$ W/Hz, L is the system losses, SNR_{Ro} is the required output signal-to-noise ratio for target detection, $\Delta f = 1/t_m$ is the filter width, R is the range from radar to target, and σ is the target RCS. For this simulation, the resultant peak power for detecting the warship at 21 km is 10.5W (10 dBW), as shown in Figure 13. This value is less than what an actual missile would have as the radar model operates at 4 GHz carrier frequency, whereas a real system operates at around 9 GHz. The simulation chooses a lower frequency due to the constraints of the computing power of the hardware.

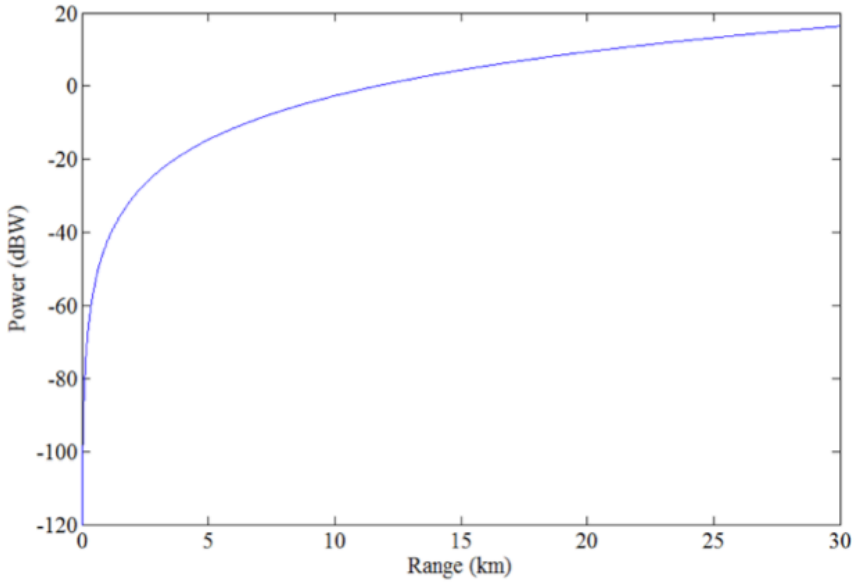

Figure 13. Radar transmitted power with respect to range-to-target.

The peak amplitude of the transmitted waveform can be approximated as

$$A_t = \sqrt{P_t} \tag{4.2}$$

The transmitted signal amplitude A_t is computed as 3.2 Volts.

In order to digitally generate the transmitting signal, the digital sampling rate must be at least twice as much as the maximum signal frequency according to the Nyquist theorem. In the case of triangular modulation, the maximum frequency is the sum of the carrier frequency, half of the modulation frequency and the maximum Doppler shift. The signal generation rate f_{SigGEN} is thus

$$f_{SigGEN} \geq 2(f_c + \frac{\Delta F}{2} + \frac{2V}{\lambda_c}) \tag{4.3}$$

From the given parameter setting in Table 6, the maximum frequency of the signal is approximately 4.01 GHz. According to (4.3), f_{SigGEN} is chosen to be 8.02 GHz.

The transmitter model generates an array of complex values using the triangular modulation equations, (2.2) and (2.6) through (2.8), which are rewritten in discrete format as

$$f_{t1}(n) = f_c - \frac{\Delta F}{2} + \frac{\Delta F}{t_m} n \cdot t_{SG} \tag{4.4}$$

$$f_{t2}(n) = f_c + \frac{\Delta F}{2} - \frac{\Delta F}{t_m} n \cdot t_{SG} \tag{4.5}$$

$$S_{t1}(n) = A_t \exp\left\{ j2\pi \left[\left(f_c - \frac{\Delta F}{2} \right)(n \cdot t_{SG}) + \frac{\Delta F}{2 \cdot t_m}(n \cdot t_{SG})^2 \right] \right\} \tag{4.6}$$

$$S_{t2}(n) = A_t \exp\left\{ j2\pi \left[\left(f_c + \frac{\Delta F}{2} \right)(n \cdot t_{SG}) - \frac{\Delta F}{2 \cdot t_m}(n \cdot t_{SG})^2 \right] \right\} \tag{4.7}$$

where n is the time index operator and t_{SG} is the signal sampling period.

Using the parameters in Table 6, the output of the transmitting signal model is a complex array S_t. This output will be used in the echo power calculation and correlation process to come. For five triangular CW waveforms, the generated FMCW triangular waveform is depicted in Figure 14.

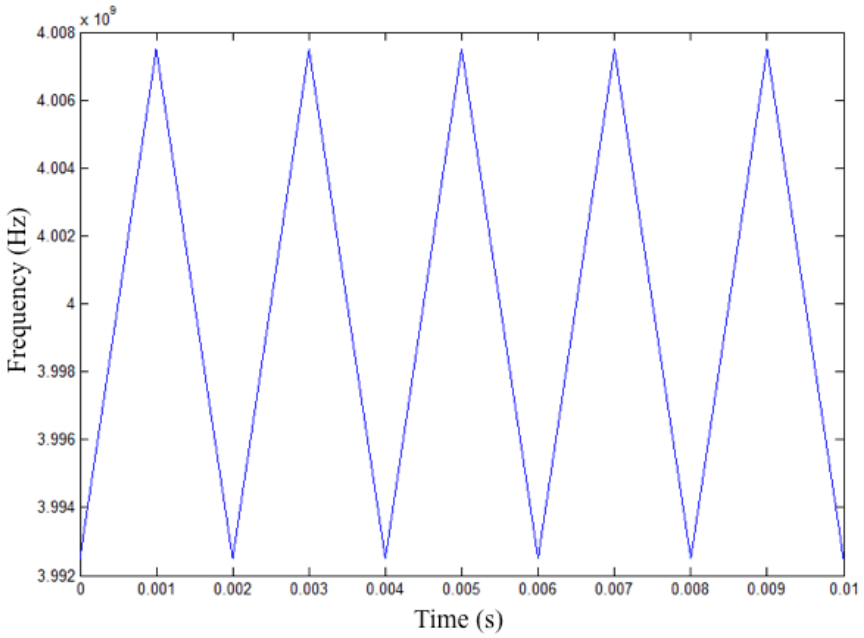

Figure 14. Simulated triangular modulation waveform with *N*=10 modulation periods.

2. Receiver Model

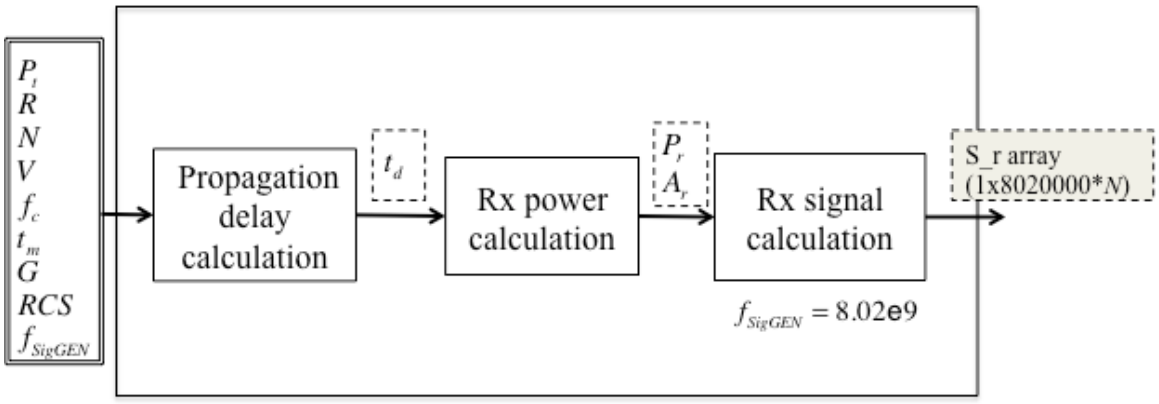

Figure 15. Received signal MATLAB model block diagram.

The receiver model block diagram is as shown in Figure 15. The receiver model is similar to the transmitted model, except the time delay and Doppler frequency are added. The Doppler frequency shift was introduced in (2.9). The propagation delay is the time required for the transmitted signal to propagate to the target and return, therefore

$$t_d = \frac{2R}{c} \tag{4.8}$$

To evaluate the echo amplitude at the receiver end, two-way signal spreading loss and target reflection gain must be considered. Two-way spreading loss is expressed as

$$L_{prop2} = -64 - 40\log(F) - 40\log(d) \tag{4.9}$$

where F is the signal carrier frequency (in MHz,) and d is the propagation distance (in km.) The signal reflected from target has additional loss (gain) of

$$L_\sigma = -39 + 20\log(F) + 10\log(RCS) \tag{4.10}$$

The signal power at the radar receiver is the sum of transmitter power, antenna gain and above losses

$$P_r(dB) = P_t(dB) + 2G - 103 - 20\log(F) - 40\log(d) + 10\log(RCS) \tag{4.11}$$

the calculated received power is -132 dBW, or 0.06 pW. Figure 16 shows the received power as a function of range being constant due to the transmitted signal power being adapted to keep the SNR at a specified level within the receiver (see Figure 13). The amplitude of the signal is approximated by (4.2), which gives 0.23 μV.

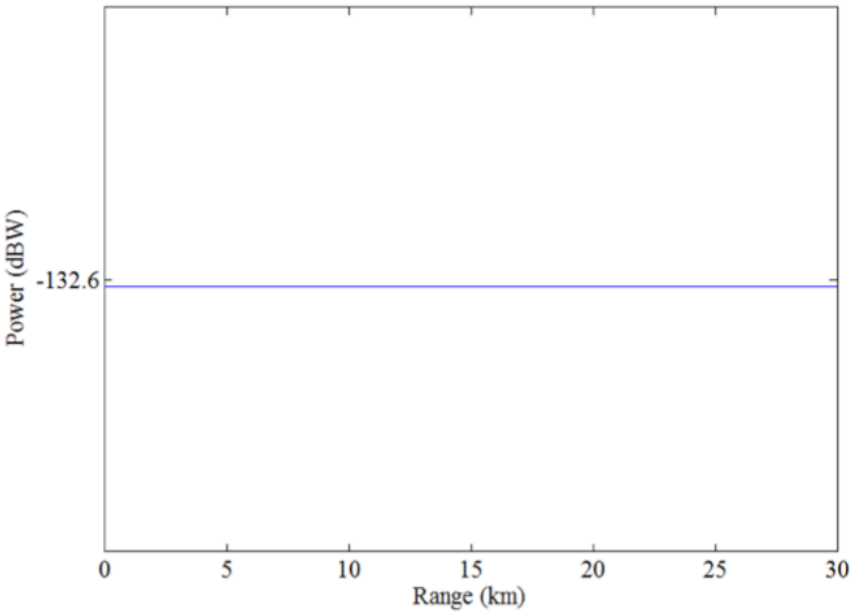

Figure 16. Received signal power with respect to range-to-target.

The received signal frequencies for up-chirp and down-chirp sections are

$$f_{r1}(n) = f_c - \frac{\Delta F}{2} + \frac{\Delta F}{t_m}(n \cdot t_{SG} - t_d) + \frac{2V}{\lambda_c} \tag{4.12}$$

$$f_{r2}(n) = f_c + \frac{\Delta F}{2} - \frac{\Delta F}{t_m}(n \cdot t_{SG} - t_d) + \frac{2V}{\lambda_c} \tag{4.13}$$

and the received waveform can then be calculated as

$$S_{r2}(n) = A_r \exp\left\{ j2\pi \left[\left(f_c - \frac{\Delta F}{2} \right) \cdot (n \cdot t_{SG} - t_d) + \frac{\Delta F}{2 \cdot t_m}(n \cdot t_{SG} - t_d)^2 + \frac{2V}{\lambda}(n \cdot t_{SG} - t_d) \right] \right\} \tag{4.14}$$

$$S_{r2}(n) = A_r \exp\left\{ j2\pi \left[\left(f_c + \frac{\Delta F}{2} \right) \cdot (n \cdot t_{SG} - t_d) - \frac{\Delta F}{2 \cdot t_m}(n \cdot t_{SG} - t_d)^2 + \frac{2V}{\lambda}(n \cdot t_{SG} - t_d) \right] \right\} \tag{4.15}$$

From above equations, the calculated transmitted and received signals can be plotted as shown in Figure 17. Note that the slopes on the modulation are parallel.

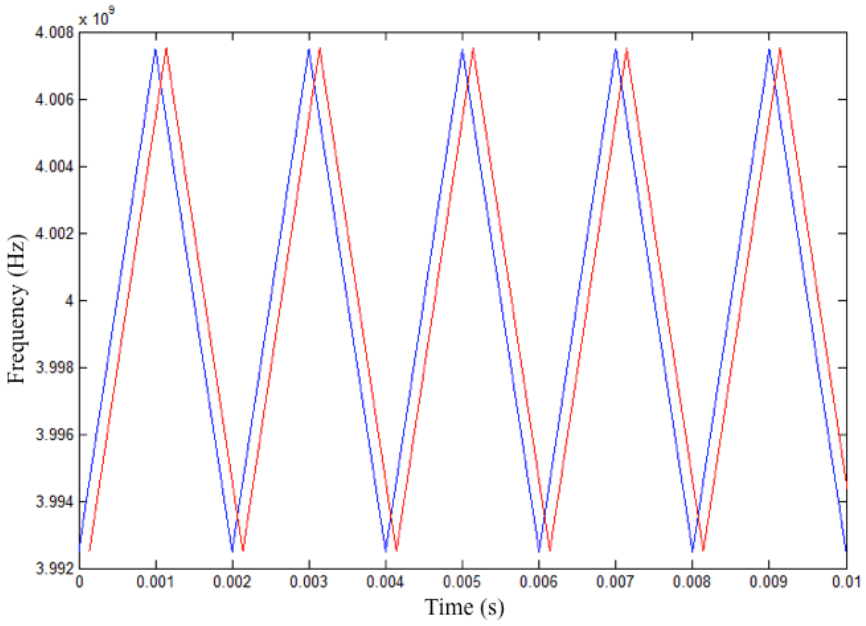

Figure 17. MATLAB simulated FMCW triangular waveform.

3. Mixer

The mixer model takes the received signal and jamming signal to correlate with the reference signal. The output of this model is the summation of both correlated signals (Figure 18). White Gaussian noise is added to the signal prior to the correlation process. The required SNR at the receiver is a constant 20 dB.

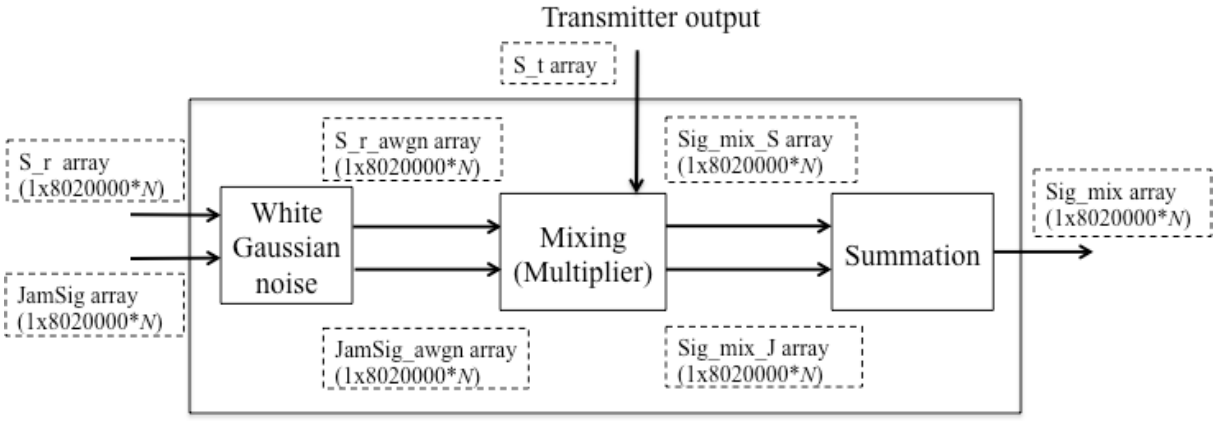

Figure 18. Mixer MATLAB model block diagram.

At the mixer, the reference signal and received signal are multiplied in the time domain. Since the transmitted signal is complex, the reference signal is the complex conjugate of the transmitted signal. The correlated signal, or beat signal, is therefore

$$S_{beat}(t) = S_t^*(t) S_t(t - t_d) \tag{4.16}$$

The asterisk above the transmitted implies complex conjugate. Same procedure applies to the jamming signal array, which will be discussed later in the chapter.

4. Low-Pass Filter

Due to the trigonometric identity regarding the sum of cosines, the product of two signals has two distinct sinusoidal components, whose frequencies are the sum and differences of the two signal frequencies being correlated [11]. The low-pass filter eliminates the higher beat frequencies as well as any noise above the filter cutoff frequency. The filter cutoff frequency is designed to match the maximum beat frequency corresponding to the maximum operational range of the radar. The maximum beat frequency $f_{b\max}$ is calculated as

$$f_{b\max} = \frac{2R_{\max}\Delta F}{ct_m} + \frac{2V_{\max}}{\lambda_c} \tag{4.17}$$

where $R_{\max}$ and $V_{\max}$ is the maximum detectable range and range rate according to the radar design. Note that value of $f_{b\max}$ mostly depends on that of $R_{\max}$, since the Doppler frequency shift is relatively small. The filter cutoff frequency is therefore

$$f_{cutoff} = f_{b\_\max} \tag{4.18}$$

The low-pass filter model (Figure 19) is a finite impulse response (FIR) filter and is built using the MATLAB *fdesign.lowpass* function in Signal Processing toolbox. The maximum detectable range of the radar model is designed to be 30 km, which gives a maximum beat frequency on the order of 3 MHz. The cutoff frequency of the filter is therefore set to be 3 MHz. The filter magnitude response is shown in Figure 20.

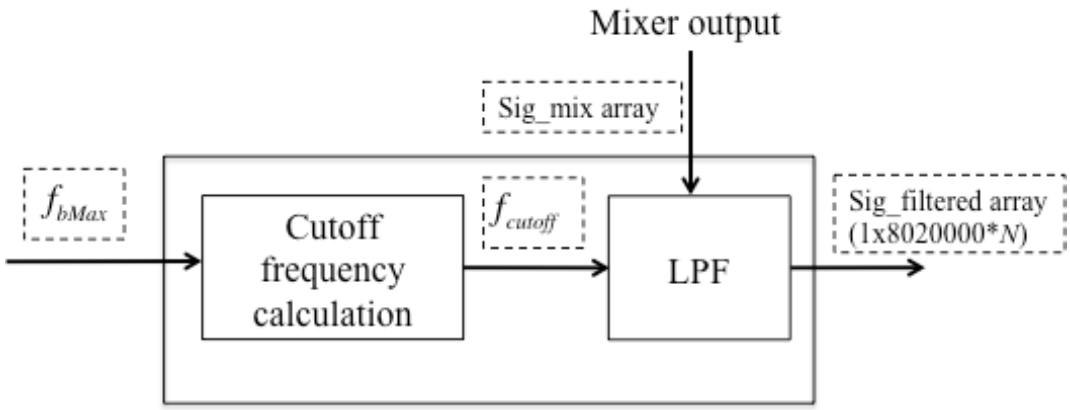

Figure 19. Low-pass filter MATLAB model block diagram.

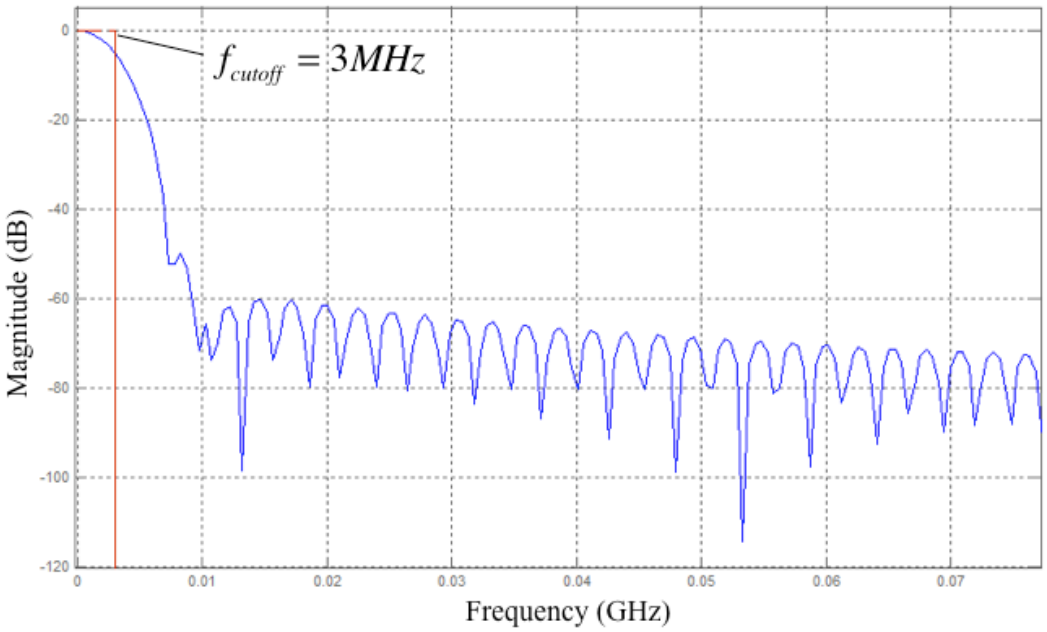

Figure 20. Low-pass filter magnitude response.

5. Digital Signal Processing

a. ADC

In the MATLAB simulation, signals are being generated and processed digitally. The maximum signal frequency being processed at this stage is significantly less than the original signal, down sampling is beneficial for simulation efficiency. The sampling frequency is chosen to be twice as much as the maximum beat frequency.

Therefore, f_s is 6.02 MHz. The ADC down conversion is achieved by sampling the beat signal array every f_{SigGEN} / f_s samples.

b. Fast Fourier Transform (FFT)

In this stage, the beat signal array is broken down and investigated individually every modulation period. Prior to the transformation, the signal array is first scaled by the Blacksman-Harris window to reduce possible Discrete Fourier Transform (DFT) leakage, which may cause strong sidelobes in the spectrum. Fourier analysis converts each individual period of signal from time domain to frequency domain, but the imaginary part of the complex signal is omitted. In order to allow the signal magnitude to be detected correctly in the magnitude detector, the complex signal of each modulation period must be transformed separately (Figure 21).

The FFT size of each section is determined by the number of samples within one coherent processing interval.

$$L = f_s t_o \tag{4.19}$$

The signal is then padded up with zeros up to the next power of 2. This can be easily done using *nextpow2* function.

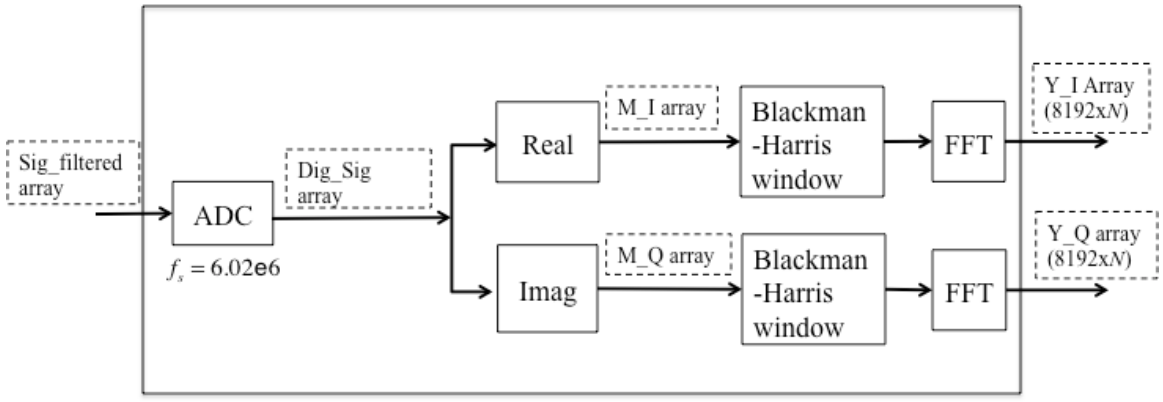

Figure 21. ADC and FFT model block diagram.

c. Envelope Approximate Detector and GO-CFAR

The FFT output of both In-phase and Quadrature channels are evaluated for combined signal envelope using the envelope approximate detector before going into the GO-CFAR model for target detection (Figure 22).

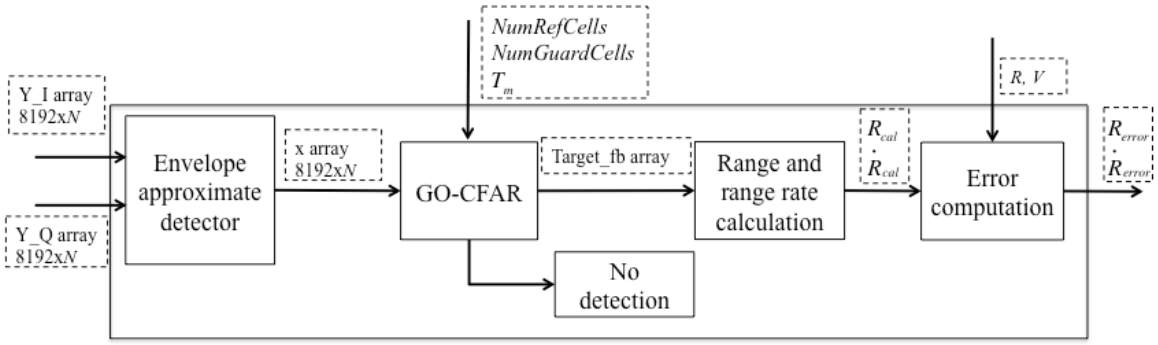

Figure 22. Envelope approx. detector and GO-CFAR model block diagram.

Using (2.1), the magnitude approximation detector has the value 1 for both constant a and b. The calculated signal envelopes of *N* periods (or frequency sweeps) are shown in Figure 23. This magnitude of the envelope is to be evaluated for target detection at GO-CFAR. With the missile approaching the target, the detected signal envelope shifts to the lower frequencies every sweep. As the range-to-target decreases with time, the envelope peak gradually shifts toward lower frequencies.

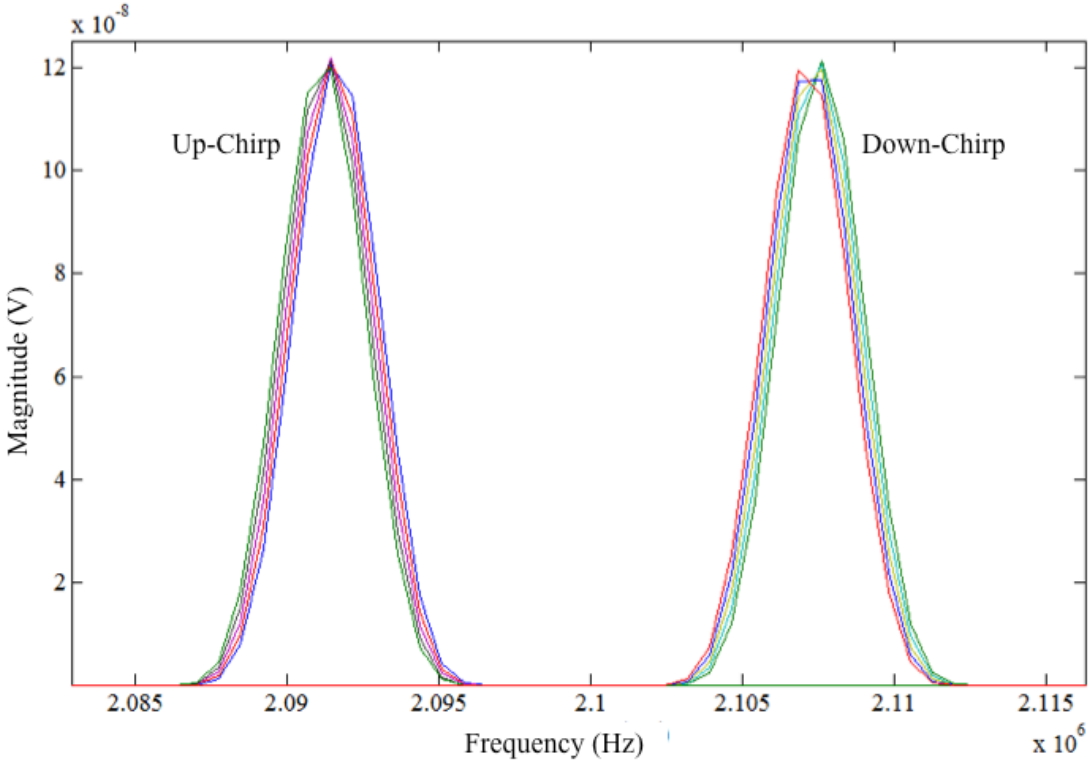

Figure 23. Magnitude detector spectrum (N=10).

The GO-CFAR model implements one guard cell and eight reference cells on each side (Figure 24). The test cell evaluates the value of the magnitude array cell by cell for detecting where signal magnitude is above threshold voltage. The choice of threshold multiplier is essential. When the chosen value is too low, much noise will be detected in the spectrum besides the target signal and causes a false alarm; with too great a threshold, the target signal may be hidden in noise. Usually the allowable PFA of a radar system is between $1e-6$ and $1e-7$. The scenario requires the PFA to be less than $1e-7$; a proper value of threshold multiplier needs to be chosen. This leads a separate test to investigate on the GO-CFAR response as a function of the number of reference cells n and threshold multiplier T_m [7].

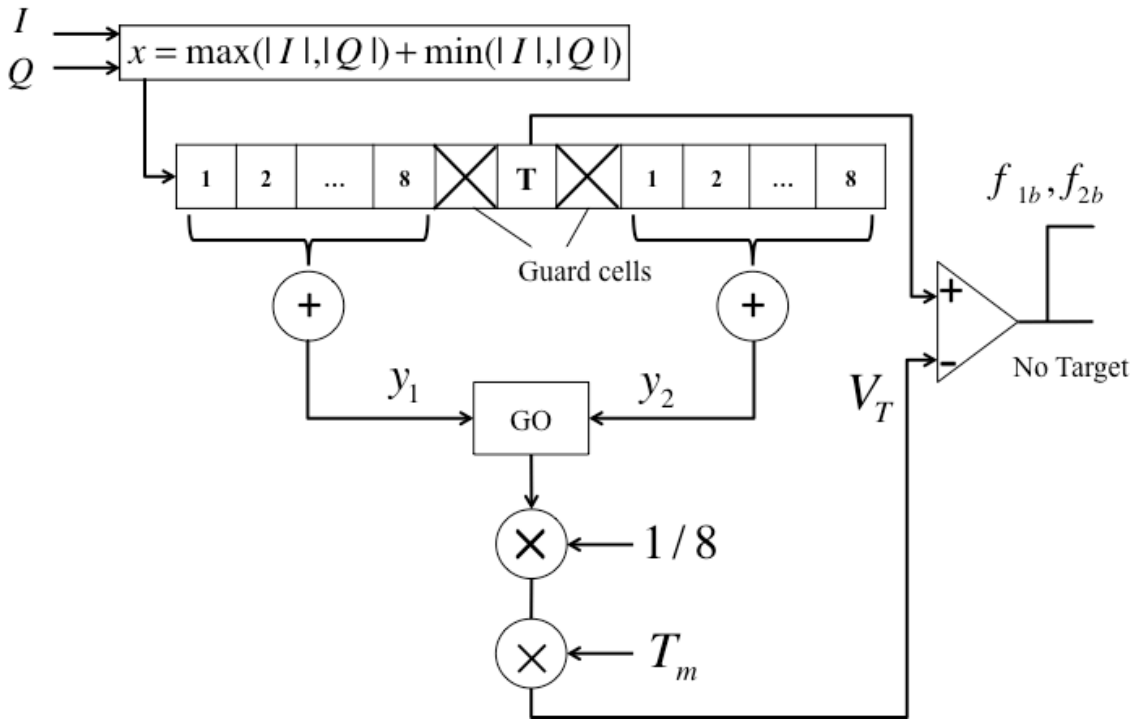

Figure 24. GO-CFAR processor with one guard cell and eight reference cells on each side.

With no target present, the noise in the magnitude spectrum can be considered as normally distributed samples with zero mean and one variance. This noise spectrum is then evaluated by a GO-CFAR detector with n reference cells and threshold multiplier T_m. From the number of detections (signal > threshold) and the total number of trials, PFA can be calculated as

$$PFA = \frac{\#\text{ of detection}}{\#\text{ of trials}} \tag{4.20}$$

A curve-fitting plot can be generated with multiple trials of various choices of *n* and T_m, as shown in Figure 25.

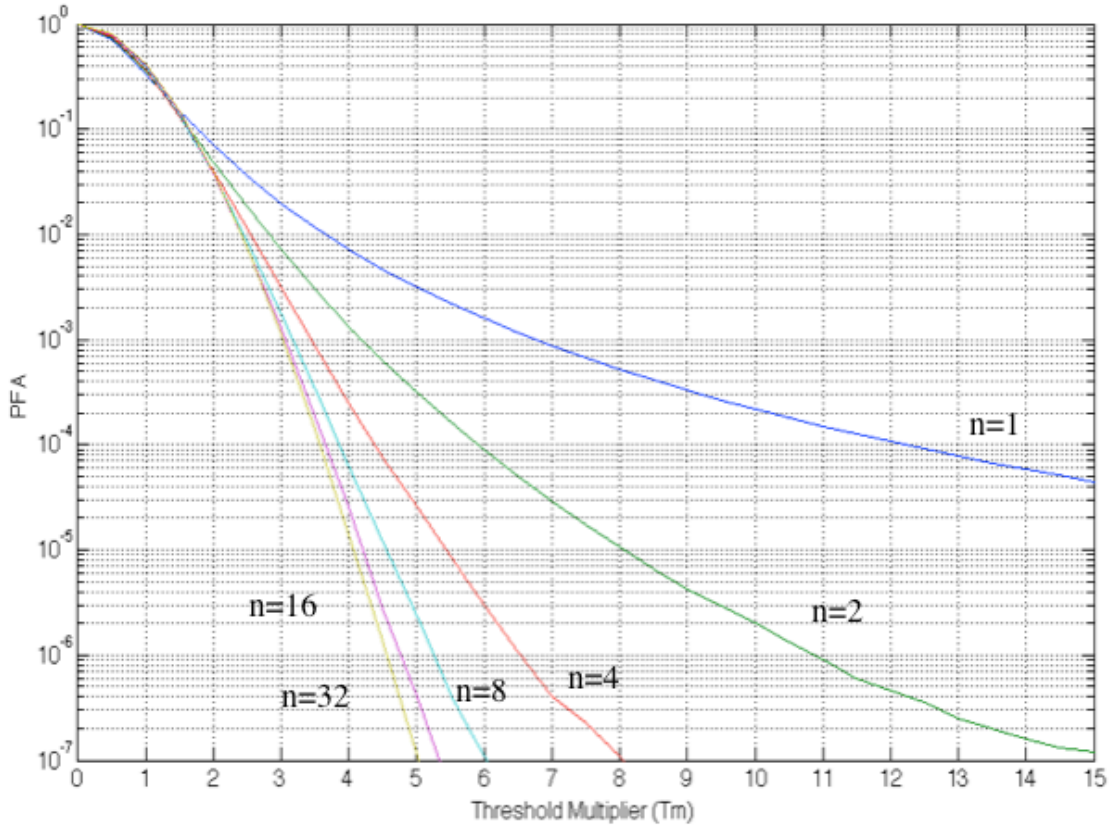

Figure 25. Envelope Approximation (a =1, b =1).

Depending on the minimum PFA allowed, the threshold multiplier can be looked up on the appropriate curve in Figure 25. For this simulation, the GO-CFAR uses eight reference cells on each side and requires PFA to be less than 10e−7. Figure 25 gives $T_m = 6$.

The GO-CFAR model returns a *Target_fb* array and *detection* array. The *Target_fb* array consists of the filter frequency where a target is detected. The *detection* array is used to show in which filters the target is present. A value of one indicates a detection and zero otherwise. The *detection* array is useful for a stem plot to give a clear visualization of target position (Figure 26).

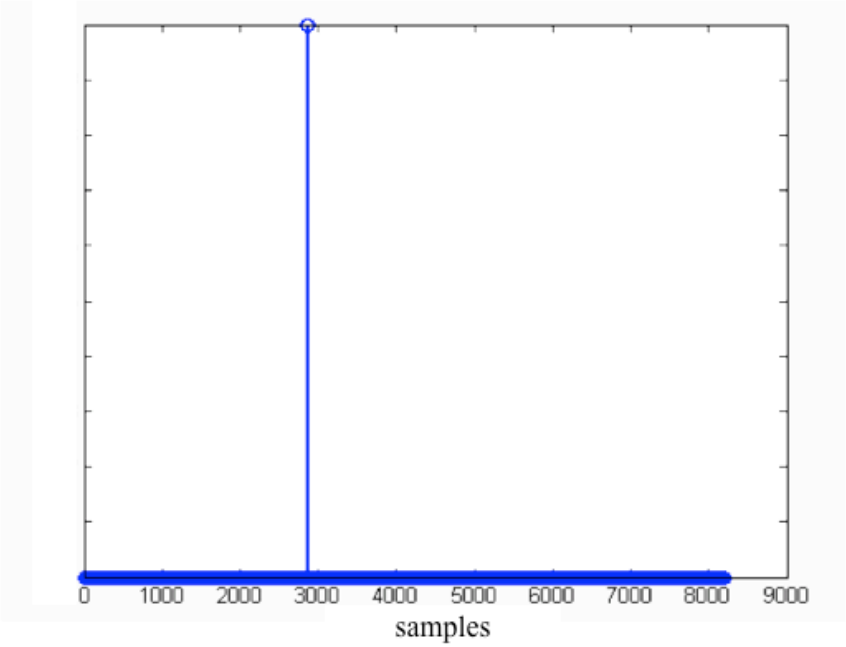

Figure 26. Target detection stem plot.

For the given scenario, a target is first detected (first triangular waveform) at bin 2847 for up-chirp periods and bin 2869 for down-chirp periods, which give f_{b1} =2,091,420 Hz and f_{b2} = 2,107,587 Hz. The beat frequency gradually reduces as the missile approaches over time. The target moves down one range bin at the fifth waveform (N=9 and 10), where target is detected at bin 2847 and 2868, giving the new beat frequencies f_{b1} =2,091,420 Hz and f_{b2} = 2,106,853 Hz. This result is used for range and range rate calculation.

d. Range and Range Rate and Error Calculation

The GO-CFAR model output, *Target_fb*, is used for range and range rate calculation. From (2.22) and (2.23), the calculated range is 20,995.04 meters and range rate is 303.13 m/s for the first detection. Compared to the input parameters (R=21,000 m and V=300 m/s) the error is computed as 4.96 meters and − 3.13 m/s. The results are satisfying since both errors are within one bin width. The second and third waveforms suggest the same result as the first one. The target was undetected on the fourth down-chirp envelope waveform by the GO-CFAR due to DFT leakage, as the target was

moving down between the range bins (Sweep 8 in Figure 27). At the fifth waveform, the calculated result is 20,991m and 289.35 m/s. The first detection result is summarized in Table 7. For comparison, the calculated range and range rate of each triangular waveform are listed in Table 8.

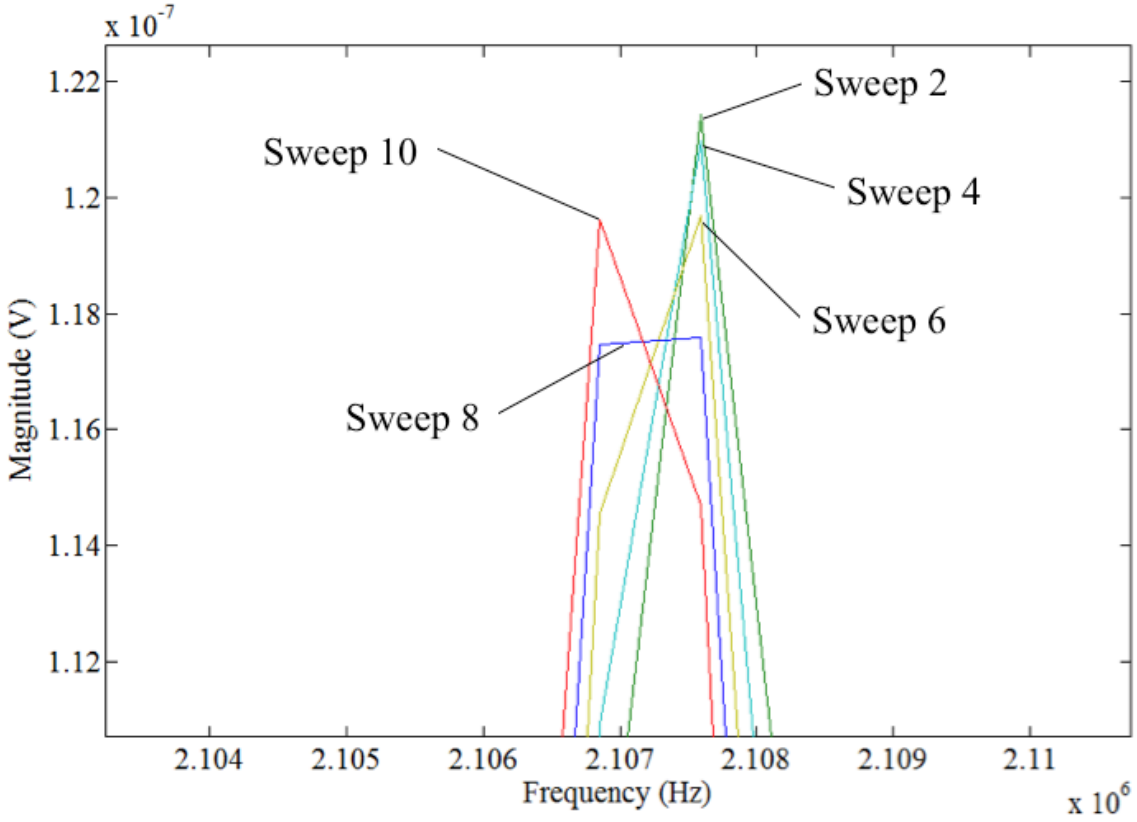

Figure 27. Signal envelope movement (down-chirp sweeps).

Table 7. Key results from simulation.

Transmter power	P_t	10.45 W
Transmitting singal amplitude	A_t	3.23 V
Received Signal Power	P_r	6.3e − 14 W
Received signal amplitude	A_r	2.34e − 7 V
LPF cutoff frequency	f_{cutoff}	3,008,000 Hz
Effective range resolution	$\Delta R'$	12.5 m
Velocity Resolution	Δv	46.87 m/s
Up-Chirp beat frequency	f_{b1}	2,091,420.90 Hz
Down-Chirp beat frequency	f_{b2}	2,107,587.89 Hz
Range to Target	R_{cal}	20,995.04 m
Range Rate	$\dot{R}_{cal}$	303.13 m/s
Target Velocity	V_t	0 m/s
Range_Error	R_{error}	4.96 m
Target Velocity Error	V_{error}	− 3.13 m/s

Table 8. Detection result by waveforms for R = 21,000 m, V=300 m/s.

Waveform	f_{b1} (Hz)	f_{b2} (Hz)	R_{cal} (m)	$\dot{R}$ (m/s)
1	2,091,420.90	2,105,787.89	20,995.04	303.13
2	2,091,420.90	2,105,787.89	20,995.04	303.13
3	2,091,420.90	2,105,787.89	20,995.04	303.13
4	2,091,420.90	undetected	X	X
5	2,091,420.90	2,106,853.03	20,991.37	289.35

C. SUMMARY

The FMCW radar model is built to emulate an actual FMCW radar signal process. The model is constructed based on an actual radar algorithm and theory discussed in Chapter II. The major strength of this model over other existing ones is its flexibility to accept various inputs and to allow for future modification. This flexibility is critical as signal jamming is a vast subject and many variables are to be tested (i.e., number of periods per scan, number of GO-CFAR guard cells, reference cells and more). Not only

can it be used for this project but this model also can easily be modified to work with other FMCW modulation (sinusoidal, sawtooth) techniques.

In the simulation performed in this chapter, the model correctly detected and evaluated the target range and speed. The next chapter discusses the resistance to jamming inherent in FMCW DSP and the possible EA techniques against it. These jamming techniques are also modeled in MATLAB to perform jamming simulation to the existing radar model. The simulation results can provide an insight into EA against FMCW radar in real world.

V. FMCW SIGNAL JAMMING

One of the major strengths of FMCW radar is its resistance to jamming signals. The FMCW radar DSP mechanism adds processing gain to coherent signals and attenuates the non-coherent jamming signals to obtain high SNR at the spectrum. This chapter investigates FMCW signal jamming by first discussing the FMCW radar jamming resistance from a DSP perspective. From there we discuss the possible jamming waveform that can overcome these disadvantages and causes of detection error. The jamming waveform model is then created and tested using the MATLAB simulation introduced in Chapter IV. The jamming effect is evaluated by calculating the change in range and range rate due to jamming. Note that in this chapter the focus is on how radar DSP will respond to the selected jamming signals. Real-world feasibility of the proposed jamming technique will be discussed in Chapter VI.

A. FMCW RESISTANCE TO INTERFERENCE

1. Correlation Process

FMCW radar implements a homodyne system, which indicates that the receiver expects a certain waveform to be processed. When a signal enters the radar receiver, it is correlated with a reference signal at the mixer. The correlating process multiplies both signals in the time domain and results in a third signal that represents the degree of similarity, or coherency, between the two signals [10]. For two identical linear modulated chirp signals, separated in time t_d, the correlated signal is a sinusoid signal with constant frequency. The coherency between two mixed signals allows the signal energy to be accumulated in the same filter of the spectrum. This gives the signal high SNR at the magnitude detection so the frequency, or beat frequency, can be detected by the GO-CFAR detector.

Figure 28 is an example that shows the effect of correlation gain when mixing two identical chirp signals. Waveform (a) indicates a simple up-chirp signal used as the reference signal, and waveform (b) is a delayed replica used as the received signal. The resultant correlated signal, shown as waveform (c) in the plot, is a sinusoid signal of

constant frequency. The FFT output of the correlated signal is shown in Figure 29. Notice that the majority of the signal power is preserved at the 4.6 MHz filter.

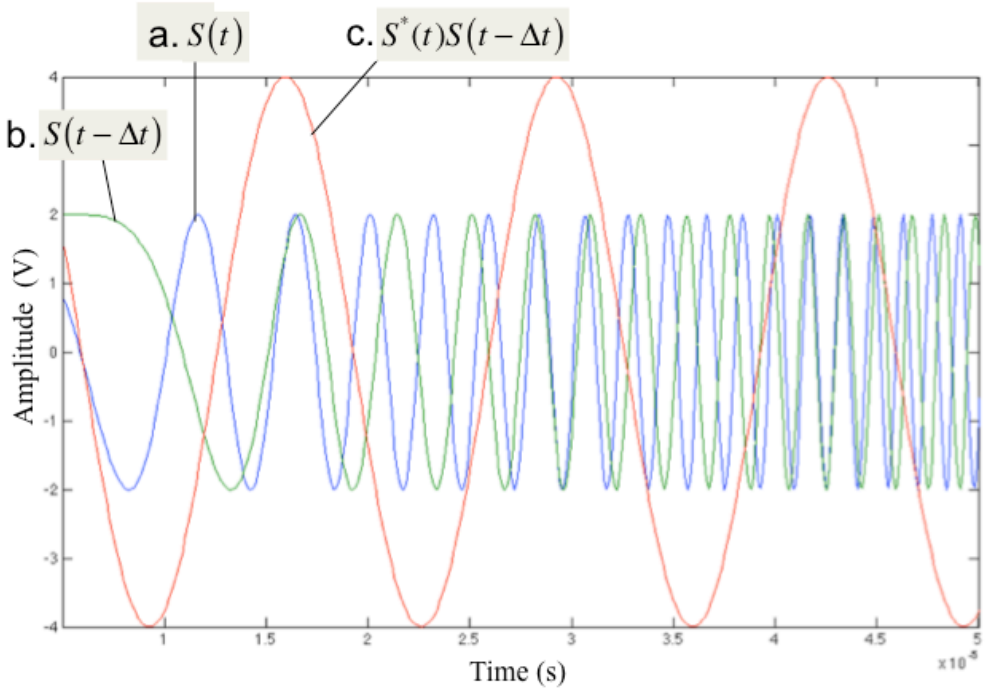

Figure 28. Correlated signal of two identical signal waveforms with time differences.

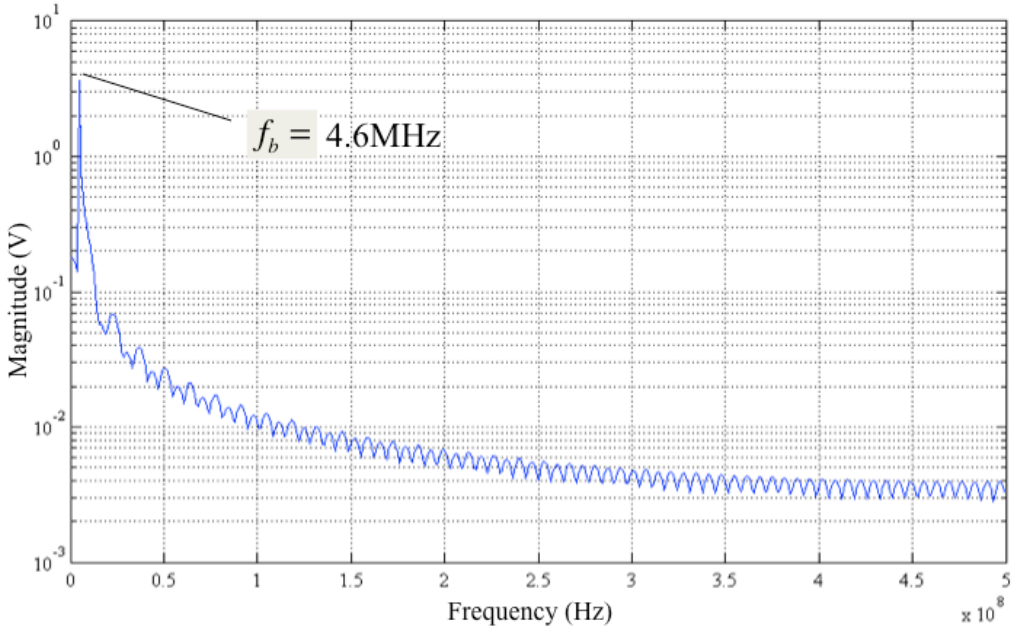

Figure 29. FFT output of correlated signal from two coherent signals.

On the other hand, when a non-coherent jamming signal is correlated, the signal power is scattered into different filters. Figure 30 is the result when correlating the same reference signal with a signal of a different chirp rate. Notice that the correlated signal (red) has various frequencies. At FFT output (Figure 31), it can be observed that the signal energy is distributed across 1.2 MHz bandwidth in the spectrum. Compare the signal magnitude in Figures 29 and 31; the coherent signal has a much greater peak power than the non-coherent signal after mixing. The high SNR at the spectrum reduces the possibility for the non-coherent signal from causing any jamming effect at the GO-CFAR detector.

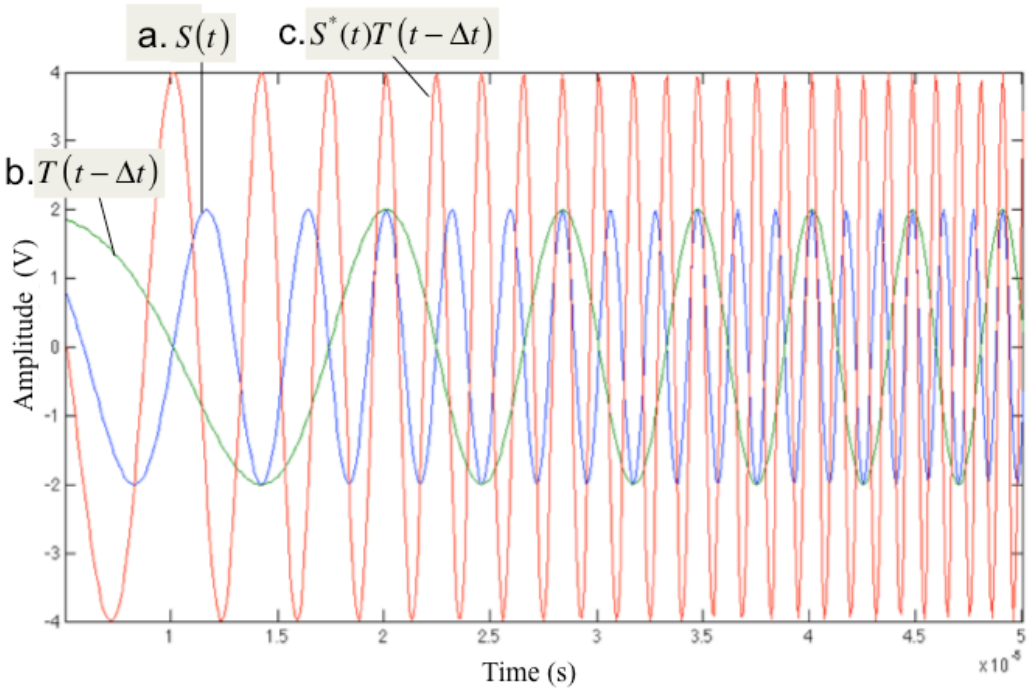

Figure 30. Correlated signal of two different signal waveforms.

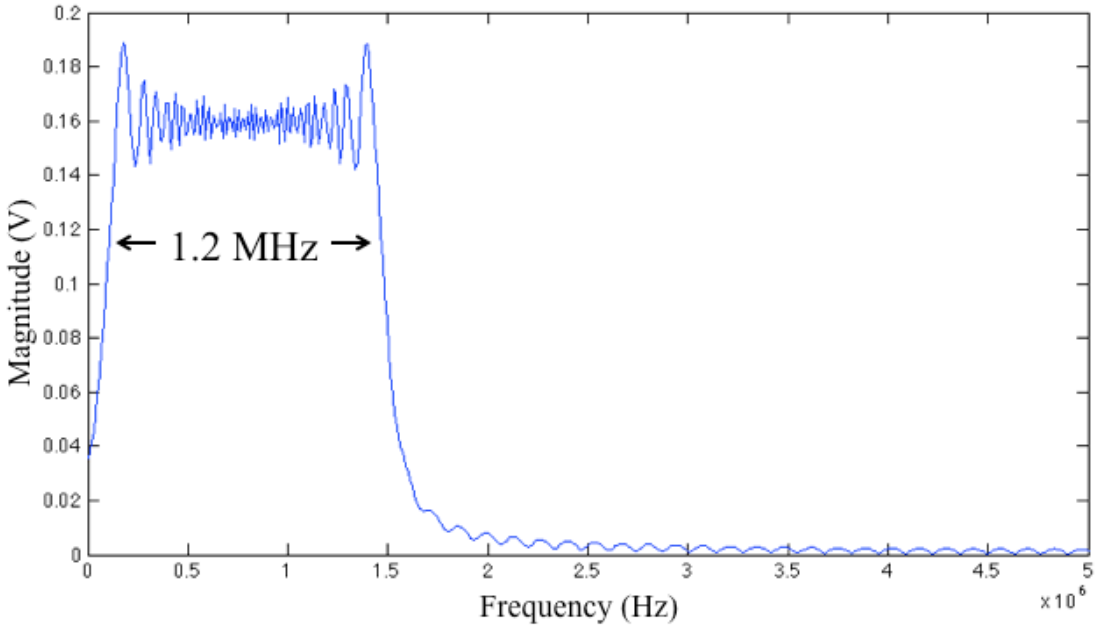

Figure 31. FFT output of beat signal from mixing non-coherent jamming signal.

In the case of random noise due to non-coherency and the spreading nature of random noise power distribution, the FFT output of the correlated signal is widely distributed across the spectrum. Therefore, it requires great input power to raise the overall noise power across the spectrum. As an example, Figures 32 and 33 depict the result when correlating the reference single with a normally distributed random noise. Noise suppression is the key for FMCW radar to operate in a noisy environment using limited power.

The above examples illustrated the edge that the coherent radar signal has over non-coherent jamming signals. For a non-coherent jamming to be successful, the jammer must have sufficient power so the jamming signal will still have enough power to cause detection error after correlation.

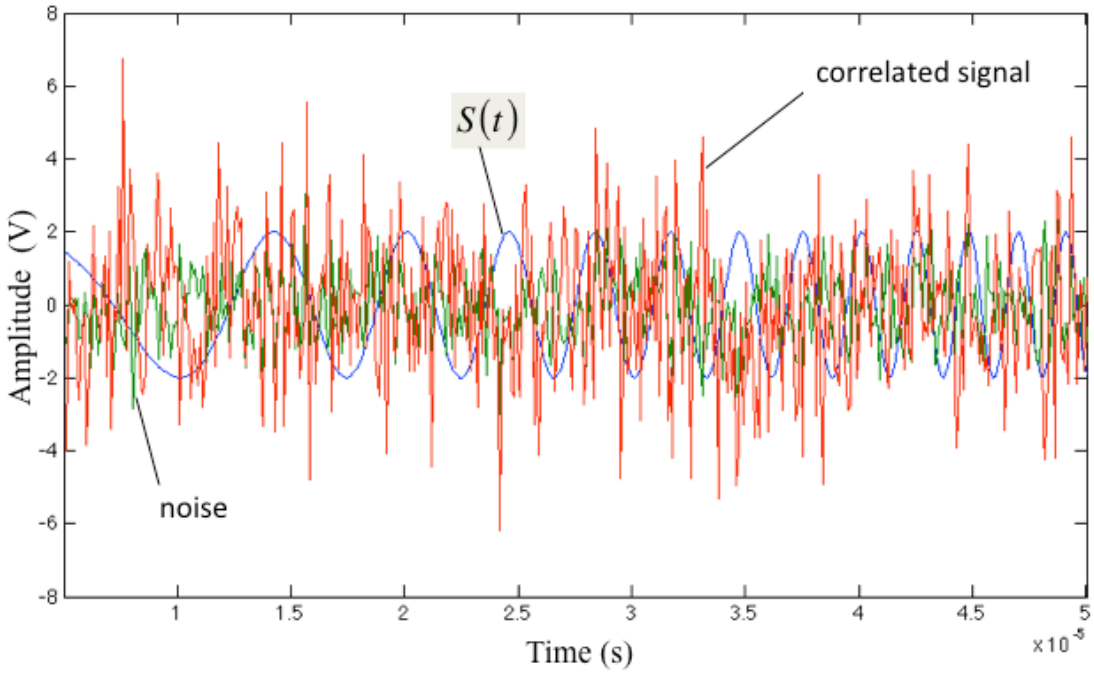

Figure 32. Correlated signal of normally distributed noise.

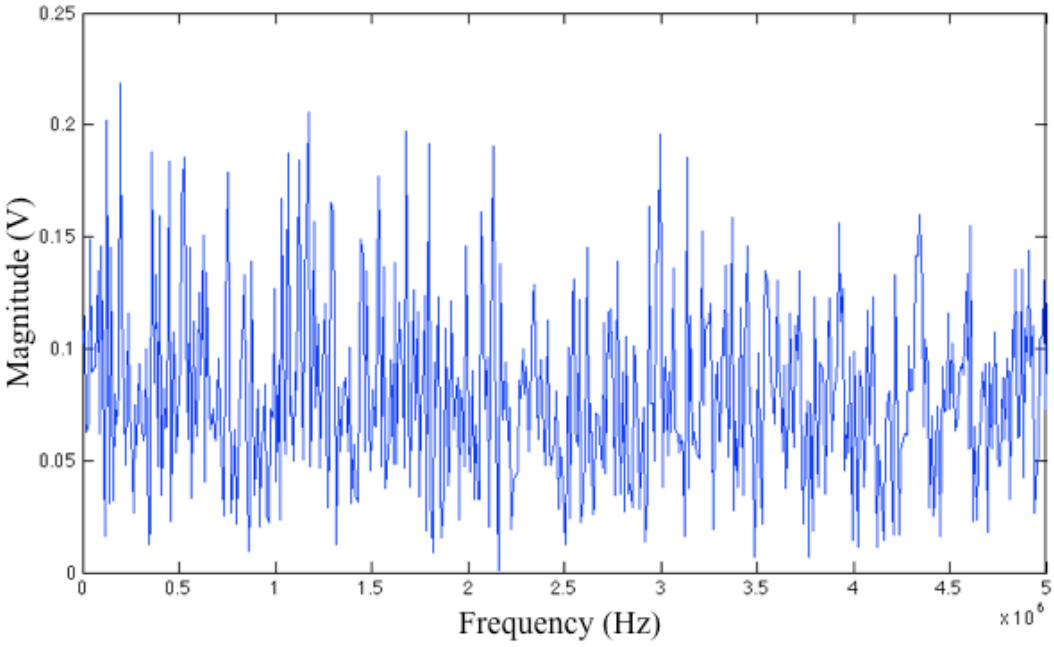

Figure 33. Correlated random noise spectrum.

2. Low Pass Filter (LPF)

The cutoff frequency of the LPF is designed based on the maximum expected beat frequency. Since beat frequency is significantly below the radar frequency band, the LPF cutoff frequency sits low in the spectrum and leaves a narrow passband. This allows only a small fraction of the received noises to pass into the FFT stage. In the case of false target jamming, if the false target signal has a time delay that is greater than the expected delay at maximum detectable range, it will be filtered out by LPF and fail to produce a false alarm to the radar.

3. Discrete Fourier Transform (DFT)

DFT has an inherent processing gain, which works similar to that of mixer correlation processing gain. Mathematically, DFT is defined as [13]

$$x(m) = \frac{1}{N}\sum_{n=0}^{N-1} x(n)e^{-j2\pi nm/N} \tag{5.1}$$

where

X(m) = the *m*th DFT output component, i.e., *X*(0), *X*(1), *X*(2), *X*(3), etc..

m = the index of the DFT output in the frequency domain, *m*=0, 1, 2, 3,..., $N-1$,

x(n) = the sequence of input samples, *x*(0), *x*(1), *x*(2), *x*(3),…,

n = the time-domain index of the input samples, *n*=0, 1, 2, 3,…, $N-1$,

N = the number of samples of the input sequence and the number of frequency points in the DFT output.

The equation can be viewed as the signal $x(n)$ cross-correlating with the signal $e^{-j2\pi nm/N}$ whose frequency is m. As noise spreads out over the frequency domain, the filter containing a target signal tone will have higher magnitude after FFT.

Also worth mentioning is that when the number of DFT input *N* increases, the DFT's output SNR will increase. This is because a DFT bin's output noise standard deviation value is proportional to $\sqrt{N}$, whereas the DFT's output magnitude for the bin containing the signal tone is proportional to *N* [13]. That being said, with a longer modulation period, the signal advantage over random noise will become more significant.

4. GO-CFAR and Power Managing

As with the GO-CFAR algorithm discussed previously, the signal amplitude detected at the test cell has to be multiple times (T_m) the average amplitude at the reference cells in order to be declared as a target. For most CFAR threshold configurations, the PFA is suppressed below $10e-6$. This gives a high threshold value to avoid the environmental noise to cause a false alarm. With sufficient noise power, the noise floor can be raised to the extent that the calculated GO-CFAR threshold voltage surpasses the target magnitude. This will make the target invisible to the detector. However, the FMCW radar power managing system will increase the transmitter power until it reaches the desired SNR, and the target will be revealed again.

Now that the FMCW radar DSP characteristics favoring the coherent waveform over others have been discussed, possible jamming strategies that work against FMCW radar are considered. The next section provides basic theories of radar jamming and later leads to what techniques may work against FMCW DSP.

B. JAMMING APPROACH AND STRATEGIES

1. Radar Jamming Overview

The goal of radar jamming is to prevent the target echo signal from being correctly evaluated at the surveillance radar receiver, or in the case of tracking radar, to interrupt the tracking sequence and allow the target to break the lock. Jamming techniques generally fall into two major categories: deception jamming and noise jamming.

Deception jamming transmits a manipulated signal that provides false target information, including false number of targets, false target range, speed and angle, to confuse the radar and affect its further action. Deception jamming can be effective against both surveillance radar and tracking radar. When used against surveillance radar, a deception-jamming system intercepts and stores the essential characteristics of the radar waveform, and then generates synthetic targets that are synchronized with the waveform pattern of the radar to create enough false targets to confuse the radar [14]. On the other

hand, when a radar tracking system locks on a target, the deception-jamming technique has the potential to break the lock by feeding the tracking circuit a synthetic target that substitutes the real target signal.

The objective of noise jamming is to inject an interference signal into the enemy's electronic equipment such that the actual signal is completely submerged by the interference [14]. Noise jamming waveforms have the advantage against search radar in that little needs to be known about the victim radar's parameters except its frequency range [14]. When the jamming noise bandwidth is less than five times more than the signal bandwidth, it is called spot jamming; otherwise, it is barrage jamming. Compared to barrage jamming, spot jamming has higher power density since the jammer power is distributed over fewer frequency ranges, which makes it more efficient in interfering with the radar passband. Barrage jamming covers a wide range of bandwidth, which increases the possibility of covering the radar passband when the radar parameters are unknown. But the trade-off is the jamming efficiency due to low power density.

2. FMCW Jamming Approach

According to what was discussed in the previous section, for a jamming signal to affect detection results, it needs to overcome the correlation gain, low-pass filtering and DFT gain, and still retain sufficient noise power at the spectrum to cause false detection at the GO-CFAR detector. Having discussed the resistance to interference of the FMCW waveform, it would be interesting to investigate how both jamming approaches, deception and noise, can affect the FMCW DSP.

a. Repeater Jamming

An effective way of generating a deception signal is repeater jamming. A repeater jammer utilizes digital radio frequency memory (DRFM) technology to store the characteristics of the intercepted radar signal and retransmit that signal again to the victim radar. Such a jamming signal has the characteristics of the radar waveform and is coherent to the radar receiver. Due to coherency, a repeater jamming signal is able to obtain the same processing gain as the real radar signal would at the radar DSP instead of

being attenuated, and it eventually creates a strong beat frequency that will be detected as a false target by GO-CFAR.

The false target behavior evaluated by the victim radar receiver can be manipulated by increasing jamming signal delay and center frequency, respectively. Knowing that the target range is proportional to the time delay of the echo signal, by adding more delay to the deception signal, the created false target will appear at a greater distance from the radar receiver. Furthermore, shifting the center frequency of the deception-jamming signal changes the differences between the beat frequencies (f_{b1} and f_{b2}) evaluated at the up-chirp and down-chirp sections. That being said, the range rate calculated by the radar computer will also change.

Repeater jamming can be effective against both the reaching and tracking mode of an FMCW radar. If multiple replicated signals of various delays can be created, multiple false targets will appear at the victim radar spectrum and create confusion for the radar. Therefore, the possibility for the real target being detected will decrease. Often the deception signal has a higher signal power that would seduce the radar tracking circuits, which makes the jamming more effective.

When the target is being locked on by the FMCW tracking mode, repeater jamming is capable of breaking lock by using a modified technique known as range-gate pull-off (RGPO). RGPO can be achieved by first making the amplified false target signal overlap the real target echo in the spectrum. When radar locks on the false target signal, it gradually increases the signal delay so the false target moves away from the real target. Once the radar tracking is pulled away with the false target to an extent, the jammer shuts off so the false target disappears. This interrupts the radar circuit and forces it to reacquire target.

Repeater jamming can easily seduce the radar tracking when a false target signal has greater power than the real target return. The high target SNR may mislead the power managing system to decrease the transmitter power, submerging the real target signal into noise. Therefore, a repeater jammer usually amplifies the signal before transmitting. Theoretically, once the false target successfully seduces the tracking system,

RGPO can work effectively against both tracking approaches, fixed-beat frequency and fixed-modulation bandwidth, as mentioned in Chapter II.

b. Noise Jamming

Unlike repeater jamming, noise jamming waveforms are suppressed at the radar receiver and thus are less efficient. The examples given in Section A have shown that non-coherent jamming waveforms receive great attenuation at FMCW DSP components and only retain a little power at the detection phase. In order to efficiently distribute jammer power into the radar detector, the jammer must have a certain degree of knowledge of the victim radar band. The more one knows about the frequency range of the radar, the more efficiently one can jam it.

Random noise waveforms are not efficient against FMCW radar. Since the jamming power is distributed across a wide range of frequencies of the FMCW frequency band, the power density is inherently small. For example, for a 150W jammer covering a 15 MHz radar bandwidth (same as the simulation model), the power density is merely 0.1 μW/Hz. With the effect of spreading loss and radar DSP, the power that reaches the GO-CFAR detector is minimal. Even if such energy is enough to reduce the SNR and temporarily affect detection, it would soon lose the edge once the radar power managing system increases the transmitter power. It is much more difficult for the jammer to increase the wideband noise power. When facing a wideband FMCW radar, a noise jammer has little chance to win the power race. This is also true for barrage jamming when the radar bandwidth is unknown.

When the radar center frequency is known, an alternative way of delivering energy into the radar receiver is through a pulse waveform that transmits noise bursts about the radar's center frequency. This compromised jamming waveform lacks the total effectiveness of the true repeater jammer and requires more knowledge of the victim radar than the true noise jammer [14]. However, the strong impulse injected into the radar's processing interval may raise the noise floor to the extent that the target signal SNR becomes insufficient to be detected by GO-CFAR. Besides, since pulse jammers

have much higher peak power than CW radar, with sufficient PRF, it may overwhelm the radar signal spectrum.

Another approach is to inject a complex sinusoid signal to the radar receiver. This technique is known as tone jamming. According to the principle of quadrature mixing, when multiplying a time series by the complex exponential $e^{j2\pi f_o t}$, the signal's spectrum is shifted upward in frequency by f_o Hz. It would be interesting to see how this effect can affect the radar detection.

The MATLAB simulation of this project tests selective jamming techniques of both deception and noise jamming approaches. These techniques include repeater jamming, Gaussian pulse jamming and carrier-tone jamming. The following section introduces the jamming signal models.

C. JAMMING SIGNAL MODEL

1. Repeater Jamming

Repeater jamming waveform has the characteristics of and is coherent with the FMCW radar waveforms. Therefore, the jamming signal is generated using the same algorithm as the received signal model except with higher signal power and additional time delay. To perform RGPO, the false target should first be placed as close to the real target range as possible to seduce the radar tracking, and then walk off the tracking system by increasing the time delay. The additional time delay that is needed for the false target to move up one range bin is

$$t_{d\_j} = \frac{\Delta R'}{c} \tag{5.2}$$

where $\Delta R'$ is the radar range bin size and c is the speed of light. Given that the range resolution of the radar is 12.5m, t_{d_j} is calculated as 42 ns. That is, the false target will shift up by one range bin if additional 42 ns are added to the received radar signal. The simulation will run several times using different delays to observe the movement of the false signal relative to the real target.

Velocity deception can be created by shifting the signal center frequency. Given that the ship has ground speed of zero, the desired false velocity is, say, 15 m/s moving away from the missile. This false velocity can be injected by shifting down the signal carrier frequency by the corresponding Doppler frequency, such that from the victim radar's point of view, the false target is approaching at a speed slower than real target.

Repeater jammers amplify the jamming signal before retransmitting. In this model, the jammer power is determined by adding an additional 10 dBW to the intercepted signal power. The radar signal power at intercept receiver is calculated as the radar power with spreading loss

$$P_{jr}(dB) = P_t(dB) + G + G_i - 32 - 20\log(F) - 20\log(d) \tag{5.3}$$

where $P_t(dB)$ is the radar signal power at the transmitter; G is the gain of radar antenna; G_i is the antenna gain of the intercept receiver; F is the radar carrier frequency (MHz) and d is the range to target (km).

The jammer power is 10 dBW higher than the intercepted signal power, as

$$P_j(dB) = P_{jr}(dB) + 10 \tag{5.4}$$

Similarly, by adding one-way spreading loss, the jamming signal power at the radar receiver can then be calculated as

$$P_{rj}(dB) = P_j(dB) + G_j + G - 32 - 20\log(F) - 20\log(d) \tag{5.5}$$

Under the same ASCM scenario in Chapter IV, the simulation parameters are computed and summarized in Table 9.

Table 9. Repeater jamming model parameter.

Jammer power	P_j	1.7e−5 W
Jamming Power at Receiver	P_{rj}	2.77e−12 W
Carrier frequency	f_c	4 GHz
Modulation period	t_m	1.0 ms
Coherent processing interval	t_o	800 μs
Effective modulation bandwidth	$\Delta F^{'}$	12 MHz
Applied signal delay	t_{false}	50-500 ns
Applied doppler shift	$f_{d\text{shift}}$	−400 Hz

2. Gaussian Pulse Jamming

The pulse-jamming model generates a Gaussian pulse train using the built-in MATLAB functions *pulstran* and *gauspuls*. This Gaussian pulse function is able to generate a band-limited pulse signal according to a specified center-frequency and bandwidth. The pulse signal has a center frequency of 4 GHz. Assuming the radar bandwidth is unknown to the jammer, the jammer bandwidth is set at 200 MHz. The peak power of the pulse is arbitrarily chosen as 15W. The PRI is chosen to be 0.0005 seconds, which makes five pulses in a modulation period. Table 10 lists the parameter of the Gaussian pulse jamming model. The produced pulse waveform is illustrated in Figure 34.

Table 10. Gaussian pulse jamming model parameter.

Pulse peak power	15 W
Jamming Power at the Received	2.44e−6 W
PRI	0.2 ms
Center Frequency	4 GHz
Signal Bandwidth	200 MHz

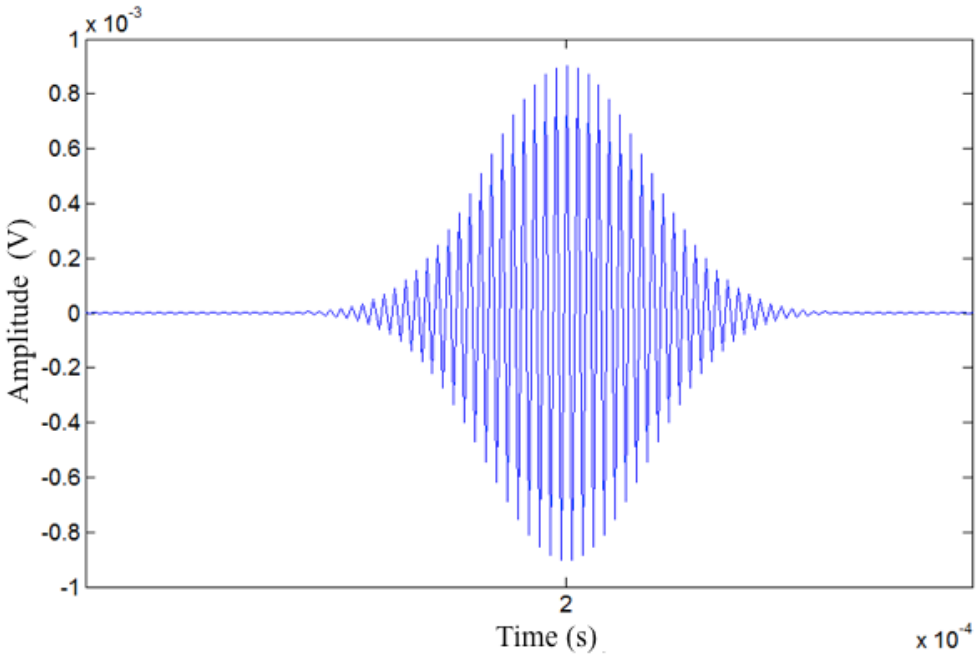

Figure 34. Gaussian pulse jamming waveform.

3. Tone Jamming

The tone jamming signal is a complex sinusoid waveform generated using the *dsp.SineWave* object and *step* function. The frequency of the sine wave is set at the radar center frequency, 4 GHz, for the best result. The power of the signal is arbitrarily 5W, which is only half of the emitter power.

D. SIMULATION RESULT

1. Repeater Jamming

Recall the ASCM scenario mentioned in Chapter IV. Having detected the missile FMCW waveform, the warship deploys repeater jamming to the missile receiver at distance of 21 km. In the MATLAB simulation, the jamming signal generated from the repeater jamming model is applied to the existing radar model. Figure 35 depicts the radar magnitude spectrum with the presence of the false target signal of 50 ns delay.

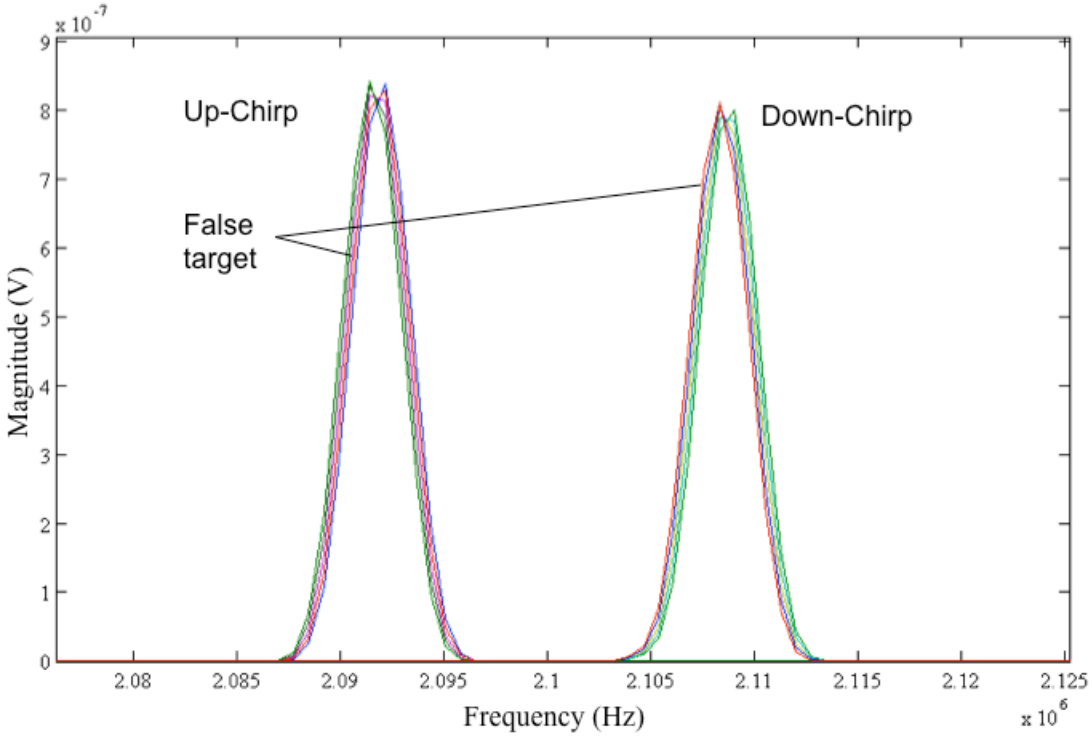

Figure 35. Radar Magnitude Spectrum with false target (50 ns shift).

In Figure 35, the false target signal appears at the filter that is one bin up from the real signal. Since the real target signal has less magnitude than the false target signal, it is buried in false target sidelobes. In GO-CFAR detection, the false target signals are successfully detected at 2,092,891 Hz for up-chirp period and 2,107,588 Hz for down-chirp period, leaving the real signal undetected. This indicates that the FMCW radar will acquire and lock on the false target instead of the real target. The range and range rate are calculated using (2.22) and (2.23), giving the result of 21,002.39m and 275.57 m/s. Given that the actual range is at 21,000m and ship velocity is zero, the calculated range and ship velocity is 2.39m and 12.27 m/s respectively. The result indicates that the repeater jamming technique has successfully injected a false target that appears to be located at further range and is moving away from the missile.

As the missile approaches the warship to a close range, the warship deploys RGPO technique in order to avoid missile strike. Given that the missile is locked on to the false target, the warship can walk off the seeker lock by increasing the repeater delay. Figure 36 is the jamming result of 500 ns repeater delay time when the missile is 1,200

meters from the warship. It can be observed that with increased repeater delay, the false target is move out from the real target position. With higher SNR than the real target signal, the false target is detected by GO-CFAR at 119,783 Hz and 134,480 Hz, whereas the real target is ignored. The computed false target range and range rate is 1,271m and 276 m/s. This result suggests a range error of 71 meters and range rate error of 24.43 m/s. In case of real world application, the repeater jammer will shut off at this time, forcing the seeker to return to search mode. The simulation simply demonstrates the false target pull-off effect in the spectrum. Chapter VI will discuss the real-world application thoroughly.

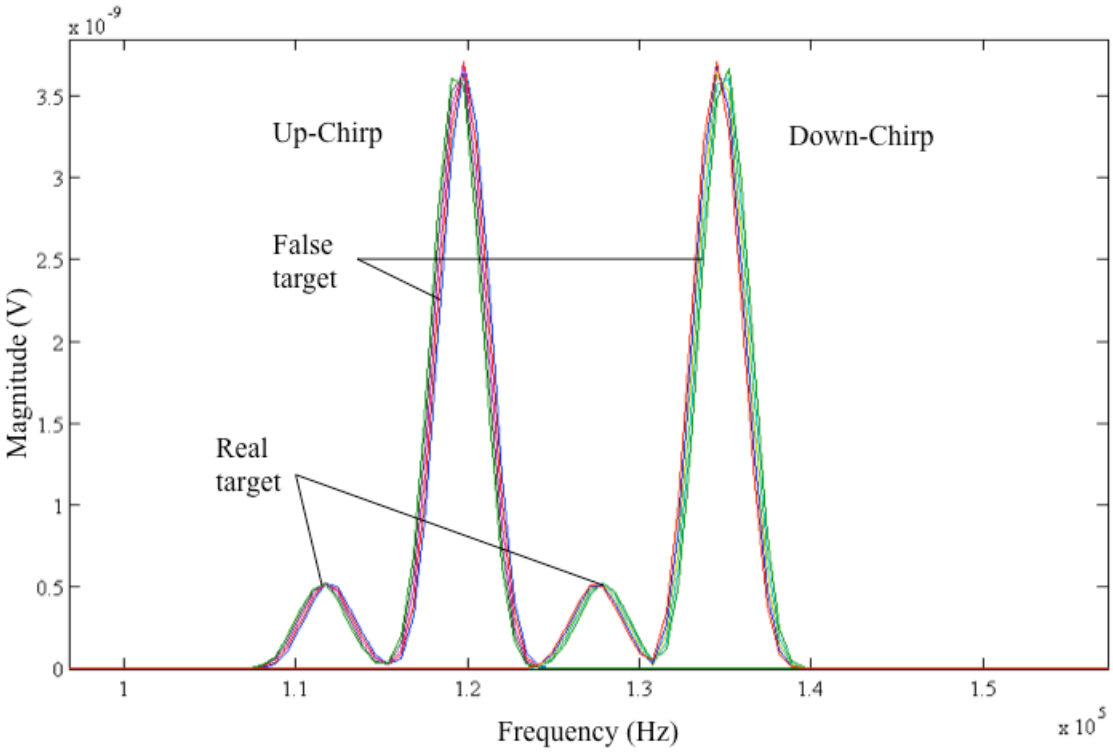

Figure 36. Radar Magnitude Spectrum with false target (500 ns shift).

2. Gaussian Pulse Jamming

The pulse-jamming signal successfully raised the noise floor and decreased the signal-to-noise ratio enough to deny target detection. Although the noise does not bury the signal completely, its power level was able to build up the GO-CFAR threshold

voltage to surpass the target signal (Figure 37). Remember that the peak power of the pulse waveform is merely 15W, which is a moderate assumption for a pulse jammer. The pulse jamming waveform can fight against the FMCW power managing by increasing pulse power or PRF.

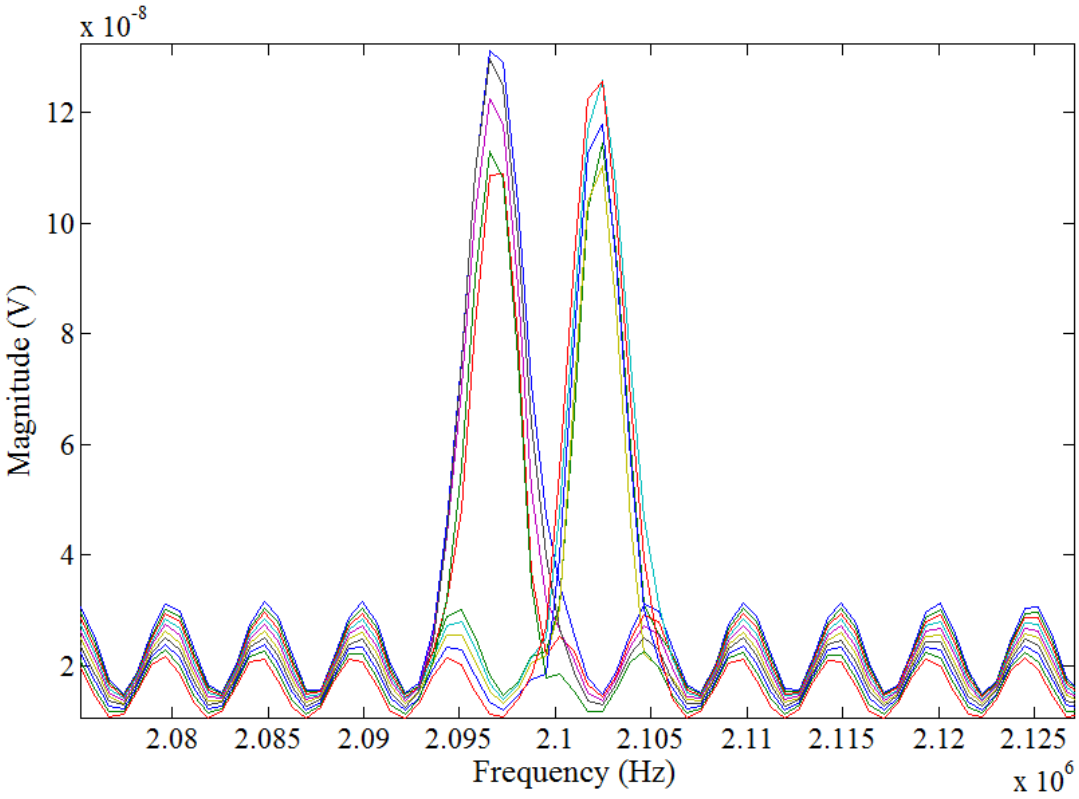

Figure 37. Gaussian pulse jammed spectrum.

3. Tone Jamming

The tone-jamming signal successfully raised the noise floor and completely buried the target signal for both up-chirp and down-chirp periods, as shown in Figure 38. Compared to pulse jamming, the tone signal can completely overwhelm the receiver with much less power. The fact that the 5W jamming signal is able to overwhelm a 10W radar makes it very efficient. Also, with the one-way propagation advantage, it is easier for the jammer to increase power against FMCW emitter power management. However, the specific simulation result does not reflect the real-world case.

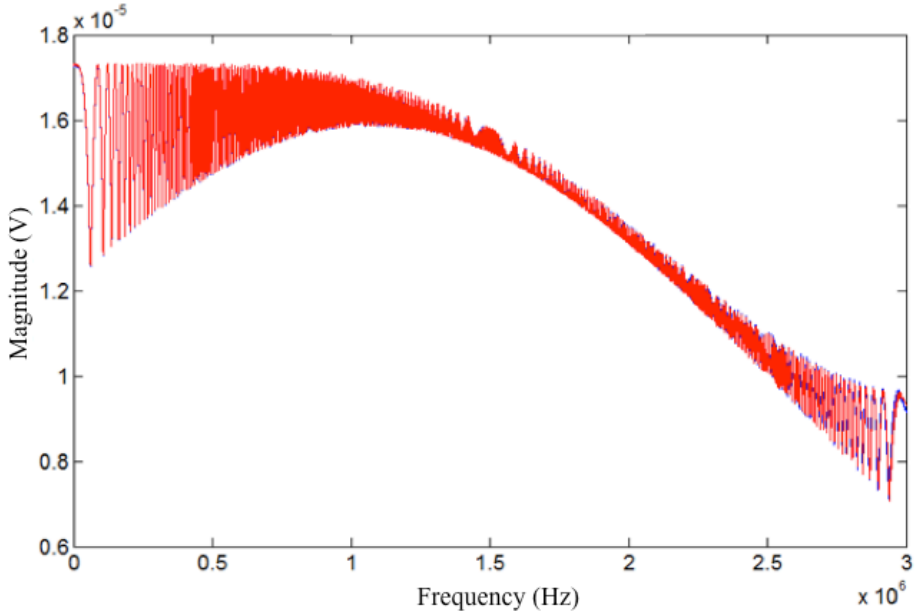

Figure 38. Tone-jammed spectrum.

After reconsidering the principle of digital signal processing, it is found that the significant noise depicted in Figure 38 is a result of a special condition in the simulation model. Again, from the quadrature mixing principle, when a signal $x(n)$ is multiplied by a complex sinusoid signal $e^{i2\pi f_o n t_s}$, the signal is shifted up by f_o in the frequency domain [13]. Therefore, when the reference signal is mixed with the 4 GHz tone, it is shifted up by 4 GHz in frequency domain. However, in discrete spectrum, for a band-pass signal located at f_o in the spectrum, a replication can be found at frequencies $f_o + kf_s$ [13], as shown in Figure 39(a). In this simulation model, since the sampling frequency (8 GHz) happen to be twice as much as the carrier frequency (4 GHz). When the reference signal is moved up from 4 GHz to 8 GHz, a DSP replica is also moved up from -4 GHz to 0 GHz. This shifting centers the alias to the baseband, where the signal is then processed by the radar model and causes significant noise effect. Figure 39(b) depicts such characteristics of the discrete spectrum. In the real-world application where mixing is implemented in continuous spectrum, aliases do not exist. In such case the correlated signal is shifted up and filtered out by the low-pass filter and creates no jamming effects.

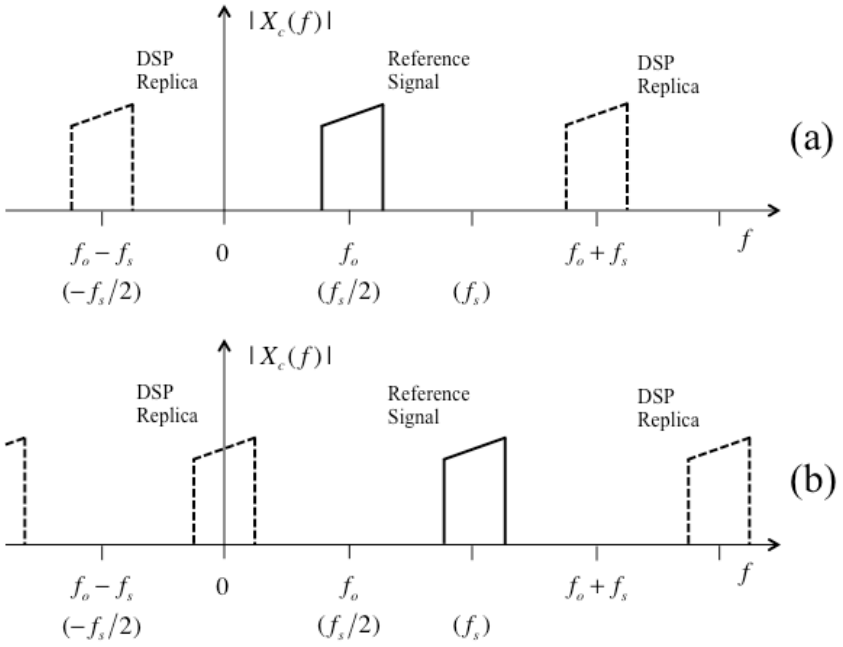

Figure 39. Discrete spectrum aliasing of (a) original bandpass signal (b) signal after quadrature mixing with $e^{j2\pi f_o t}$.

E. SUMMARY

The simulation model demonstrated the jamming effect of deception jamming and denial jamming against FMCW radar. By transmitting a signal that is coherent to the radar waveform, the jammer can successfully penetrate the radar signal processing mechanism and create a strong false target at the radar spectrum. The false target can confuse the missile seeker at the searching phase. With proper adjustment of jamming signal delay and frequency, the ship can execute RGPO, where the false target can substitute seeker lock-on and walk it off from the real target. By turning off the jammer temporarily, the seeker is forced to switch back to search mode and restart a searching sequence, which provides time for the ship to execute protective measures (i.e., maneuvering, chaff cloud). In modern electronic warfare, repeater jamming is carried out using DRFM technology. Chapter VI provides more discussions on the application side of the study.

For noise jamming, both Gaussian pulse and single tone jamming are tested and compared for efficiency. As expected, the pulse jamming signal receives significant

attenuation at receiver DSP, but the strong impulse injected to the radar passband was sufficient to decrease the target SNR and avoid GO-CFAR detection. With the advantage of one-way propagation and stronger jammer power, pulse jamming has the potential to defeat the power managing system of FMCW radar and overwhelm the radar receiver. The key for implementing pulse jamming is that the impulse must cover the radar passband; otherwise it will cause no interference to the radar detection.

On the other hand, tone jamming overwhelmed the receiver and denied detection in the simulation. The effectiveness of tone jamming is due to alias signal shifting in the digital quadrature mixing process. It is not feasible in real-world applications.

In conclusion, when the parameters of FMCW radar signal can be determined, repeater jamming is effective against both radar searching and tracking modes. In cases when only radar carrier frequency is available, a pulse-jamming signal targeting the radar frequency band can inject strong impulse to the receiver and reduce SNR.

Using the MATLAB model, we observed how a standard FMCW DSP would respond to different types of jamming signals. However, in real-world EW applications, many factors need to be considered besides the standard FMCW DSP discussed above. For example, modern radar systems implement several DSP algorithms that help identify real targets from false targets, as well as locating noise jammers for counter-attack. Chapter VI discusses these important issues and concerns that may affect FMCW jamming effectiveness.

VI. FMCW SIGNAL JAMMING IN REAL-WORLD EW SCENARIO

The MATLAB simulation results suggest that repeater jamming and band-limited pulse jamming can both be effective against the FMCW waveform. However, another great challenge of electronic attack against FMCW radars is to detect, identify and classify modern LPI radars. The LPI nature of FMCW radars makes it difficult for the opponent to be aware of the existence of LPI transmissions. Also, modern LPI radars use very complicated modulation algorithms to prevent detection and jamming. Thus, the jammer architecture has to be much more complex and capable in order to handle such complicated modulations. Lastly, many radars implement EP measures that can significantly reduce the effectiveness of repeater and noise jamming.

This chapter discusses the requirements of implementing repeater jamming and band-limited noise jamming, as well as some radar algorithms that are problematic to both jamming techniques. Also discussed are the challenges to modern EA systems from LPI emitters, before leading to a brief overview of the trends in EA system development.

A. JAMMER ARCHTECTURE REQUIREMENTS

1. Repeater Jamming

a. Wide-Bandwidth Signal Processing

The effectiveness of repeater jamming highly depends on the DRFM architecture of the EA jammer. DRFM memorizes the intercepted waveform characteristics and applies different deception techniques before retransmitting to the victim radar from which the intercepted signal was transmitted. However, when dealing with wideband radar, such as FMCW, the ADC clock speed and DRFM bandwidth must be sufficient so the intercepted wideband signal can be properly sampled and registered to the digital memory. If the input signal bandwidth is greater than DRFM bandwidth, the reconstructed signal would have errors that affect jamming efficiency. Techniques such as series-parallel sampling and shift register can help increase DRFM bandwidth using low-speed memory components without losing signal resolution [14]. Series-parallel

sampling (Figure 40) employs a tapped delay line, with taps at $\Delta t = 1/f_s$, such that multiple sample points can be taken simultaneously. For example, if five taps (five ADCs) are employed, a 500-MHz DRFM can needs to have circuitry that operates at only 100 MHz while maintaining high resolution (bits of ADC). The drawback is the hardware complexity.

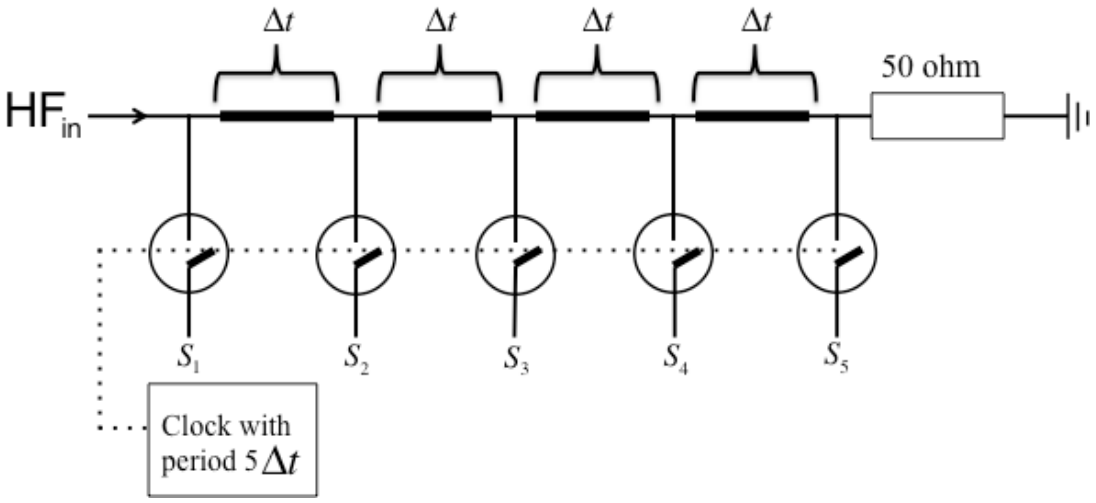

Figure 40. Series-parallel sampling technique (from [14]).

Another technique that allows lower component bandwidth is the shift register technique. This technique employs a multiple-bit ADC to reduce the required memory speed. For an eight-bit ADC, as shown in Figure 41, the required memory clock is reduced by a factor of eight. In such a case a 100 MHz signal at the ADC output can be stored in a one-bit DRFM clocked at 12.5 MHz. The series-parallel sampling technique and the shift register technique can be implemented together to process a wide-bandwidth signal with slow components.

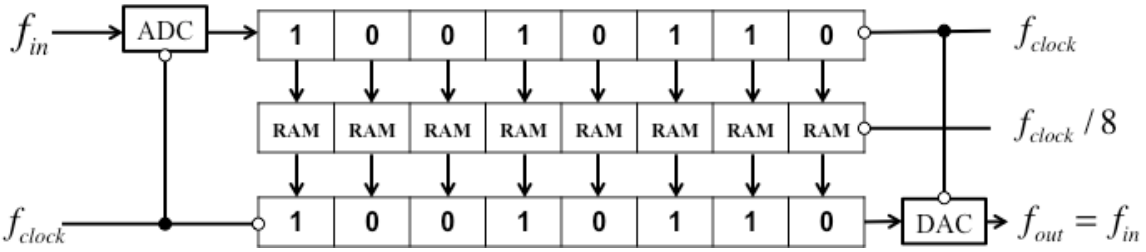

Figure 41. Shift register technique for series-parallel conversion (from [14]).

b. Knowledge of Adversary

To deploy repeater jamming, the waveform data of the intercepted signal must be available in the EA system database. Figure 42 depicts the architecture of an advanced DRFM system. Notice that the techniques generator is what determines the modulation parameters of the jamming signal. The techniques generator is designed to apply a variety of RF techniques, including RGPO and VGPO against pulsed CW and pulsed Doppler threats. It samples the RF environment and then compares it against a threat library to match specific threat identification to the received environment [14]. Without required signal data in the system library for referencing, the technique generator cannot apply proper modulation to the repeater waveform, thus the effectiveness of repeater jamming is significantly degraded. The EA system would be forced to use a generic technique rather than one specialized to exploit vulnerabilities of the specific threat.

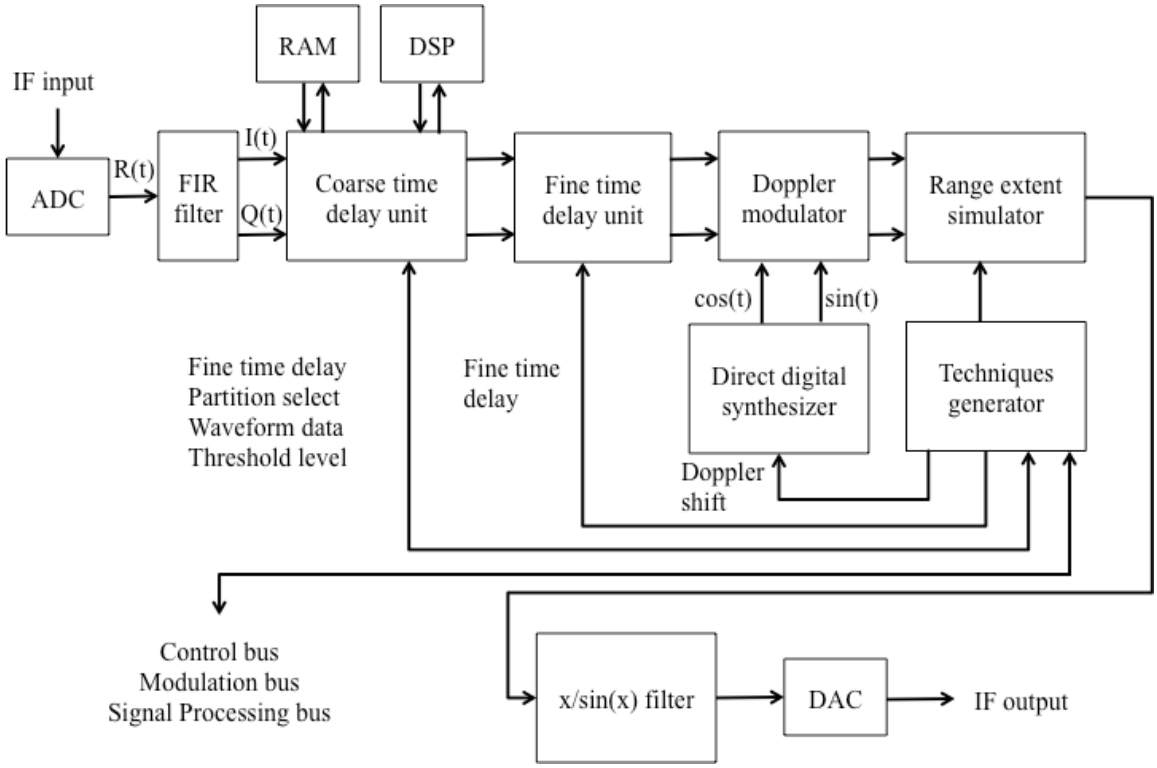

Figure 42. Advanced DRFM architecture (after [14]).

2. Band-Limited Noise Jamming

Band-limited noise jamming can be achieved by using frequency modulation to bring a baseband signal and proper carrier frequency to cover the desired frequency range. With higher PRF and high pulse power, more energy can be injected to the radar processing interval and overwhelm the receiver. Noise jammer architecture is less complicated when compared with that of a deception jammer and requires less knowledge about the victim radar. However, the jammer must have knowledge about the victim radar bandwidth in order to efficiently distribute the jamming power over a targeted frequency range, as the energy delivered outside the radar receiver band is wasted.

B. ELECTRONIC PROTECTION MEASURES OF FMCW RADAR

1. Home-on-Jam

Many modern missiles implement two tracking methods: a target tracking emitter and a passive anti-radiation seeker. This is effective especially against noise jamming. In general, when being jamming by a noise jammer, the victim radar can obtain a general direction of the jamming source using jamming strobes [14]. This is especially true with LPI radar due to low sidelobes, which give a higher angular resolution. A missile system with home-on-jam (or track-on-jam) capability can track on the noise source and destroy the jammer. Therefore, a noise jammer is vulnerable when facing a home-on-jam capable FMCW emitter.

2. Doppler Cross-Referencing

Modern tracking radars equipped with Doppler functionality cross-reference the calculated target speed with detected target position. A Doppler tracking radar follows the target by using the evaluated target velocity and position to predict the new target position at the next sweep. When a target position and velocity do not match over time, the radar will evaluate it as clutter or a false target and reject the track. Therefore, for repeater jamming conducting both RGPO and VGPO, it is important for the jammer to produce a consonant false target result to successfully deceive the radar.

3. Impulse Protection Circuit

Given the victim radar parameters, a radar pulse may inject overwhelming energy into the radar receiver band. Sufficient energy may burn the radar's circuits and disable the radar completely. An impulse protection circuit implementing varistors can suppress surge power and prevent damage of the radar receiver.

4. Leading Edge Tracker

In many radar seeker designs, especially for surface-to-air missile (SAM) systems, tracking algorithms that prioritize closing targets are implemented. Such radar systems give the closest target an additional voltage gain when multiple targets are detected. This raises the required JSR for an RGPO attack to be effective. It also limits

the possible dynamic range of the delay time that can be added to RGPO. In order to prevent the turn-around time from being too long and allow the leading aircraft to be prioritized, repeater jammers must have very short turn-around times (on the order of 50-100 ns) to minimize the probability of leading edge range trackers rejecting the deceptive signal [14]. This constraint limits deception range to below 30 meters.

C. CHALLENGES AND SOLUTIONS TO ELECTRONIC ATTACK AGAINST FMCW

1. LPI Detection, Identification and Classification

What was not shown in the simulation was the ES phase of electronic warfare. Electronic Support Measures (ESM) involving LPI signal detection, identification and classification is what provides the information required for decision making in EW against FMCW radar. Electronic intelligence (ELINT) including signal modulation parameters can be derived from spectral analysis and is critical to optimize the effectiveness of an EA operation. The wideband and coherent features of FMCW waveforms allow the radar to operate in a noisy environment with very low power. In a congested EW environment where many electromagnetic signals exist, detecting FMCW signal becomes a great challenge to ES systems. In the most extreme case when the ESM fail to detect the LPI transmission, the necessary EA measure is never implemented.

To reveal LPI signals in radio spectrum, Modern ES system implements Wigner-Ville Distribution, Choi-Williams Distribution, Quadrature Mirror Filtering and Cyclostationary Spectral Analysis for the ELINT operators to visualize the signal parameters in time-versus-frequency domain. However, since the transmission of other emitters and noise affects the visibility of the signal of interest, sufficient battlefield intelligence, such as target type, capability, location or mission can help the ELINT operators' judgment and confidence in the interpreting process, hence increase the possibility of a successful EA operation.

2. Complexity of Hardware

For an LPI system in which multiple modes can be chosen, the complexity of the intercept and classification problem for the EW receiver is increased, necessarily

increasing the complexity of the system. For large platforms such as warships, EW systems that integrate an intercept receiver and complex jammer system are available. However, in the case of suppression of enemy air defense (SEAD) operations, in which proper EA must be provided to blind adversary radar systems and, if failed, the incoming missiles, the capability of onboard jammers is typically limited. To compensate for the reduced ability of single platforms, a network-centric operation using cooperating sensors, jammers and shooters is optimum.

3. Look-Through

In EA operations, observation of emitter response to the jamming signal is needed. An EA system "listens" to the victim radar to evaluate the effectiveness of the interference so it can adjust jamming strategies accordingly. In self-screen jamming, this causes an unavoidable look-through, where the jammer pauses for a short period of time to allow radar-warning receiver (RWR) to listen to the victim radar. Look-through affects jamming efficiency since it reduces the jamming signal dwell time and gives the radar an opportunity to acquire the target during look-through. For an EA system, the look-through has to be less than the time required for the radar to reacquire a target. Ideally, any amount of look-through is unwanted [1].

In a network-centric operation, jammer look-through can be eliminated as jamming and listening are carried out by different platforms. In such cases, the jammer can continuously deliver jamming power and observe the victim radar response using the information provided by the sensor network.

4. Multiple Target Jamming

In the modern battlefield, where multiple enemy emitters are present, a jammer that is capable of jamming multiple targets simultaneously is desired. Such EA systems require much power to inject energy into the various channels at which the target radars operate. Therefore, once again, besides the output power of the jammer, the knowledge for the victim emitters is very important to execute multiple-target jamming efficiently.

5. Network-Centric Electronic Warfare Requirement

In network-centric electronic warfare, the EW receivers must be able to disseminate all onboard detections in real time. Such capability is sometimes referred to as *real-time out of the cockpit* (RTOC) [1]. On the other hand, the ability to accept real time data is known as *real-time data in the cockpit* (RTIC). RTOC and RTIC are critical in a network-centric architecture in order to share and process information in real time among sensors and shooters. This requires a wideband RF transmit and receive capability of all participant platforms. Also, a wideband local network is required for each platform to process large amounts of information internally [1].

To best benefit from the network-centric architecture, the design of the network, including the numbers of platforms required, balance between sensors and shooters, and optimal topology to be deployed, needs to be carefully evaluated for different scenarios. With the possible presence of enemy EA, the network tolerance and EP measures against electronic interference also need to be considered. The concept of network-centric architecture is as depicted in Figure 43.

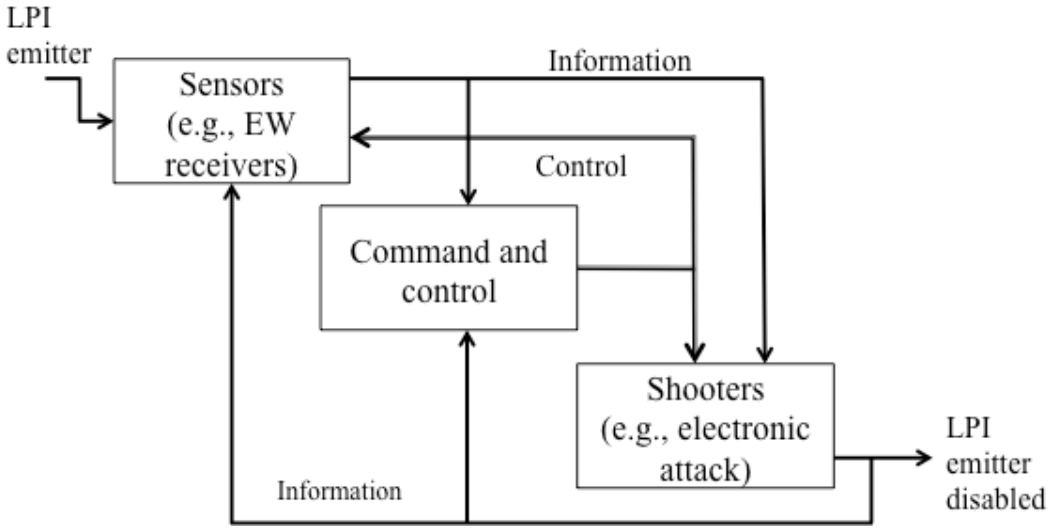

Figure 43. Network-centric architecture countering LPI emitter (from [1]).

D. TREND OF EA DEVELOPMENT

The trend of modern EA systems is network-centric architecture, where multiple sensors and shooters are incorporated under the command of a decision maker. Besides eliminating the jammer look-through as discussed previously, the network-centric architecture can utilize multiple sensors (EW receivers) to improve LPI detection. A sensor-network architecture, known as *swarm intelligence* technology, is a major approach for collecting the trace of an LPI emitter in modern EW. Swarm technology allows sharing of information among multiple sensors, thus the detections from each individual sensor are collected and evaluated as a group. This gives a higher probability of identifying LPI waveforms in a complex modern EW environment and provides the necessary information for EA measures. Swarm technology makes it possible to deploy stand-in UAVs to collect LPI emitter characteristics in enemy territories and share the collected intelligence to the decision maker and shooters for upcoming or ongoing EA operations.

As discussed previously, the key to an effective network-centric architecture is the speed with which information can be shared and processed across the network. Also, high sensitivity improves the intercept receivers' capability to identify LPI waveforms. The future digital receiver will incorporate optical technologies for speed and bandwidth, and will also incorporate high-temperature superconductors for sensitivity [1].

Specific emitter identification (SEI) technology that fingerprints the intercepted LPI emitter is currently under development. SEI can also be used for improved tracking and de-interleaving according to [1]. An EA system that implements SEI technology can have significant impact on LPI radar jamming.

E. SUMMARY

Intelligence is the key to the success of an EA operation. The development of EA and EP is the history of a tug-of-war. For every radar system there are jamming techniques that counter it. On the other hand, with the debut of new EA technologies, a corresponding EP measure is also developed. In Chapter V, it has been shown that band-limited pulse jamming and repeater jamming can work against FMCW radars. However,

most tracking radars nowadays are equipped with a home-on-jam capability that tracks on a noise source and makes the noise jammer vulnerable to such an emitter. Repeater jamming is effective against FMCW radars, but the LPI nature of FMCW makes it difficult for the target to be aware of the incoming threat. Radar algorithms such as leading edge tracking and Doppler cross-referencing also limit the effectiveness of repeater jamming. That being said, the intelligence provided by ES systems is just as important as the capability of EA system in an EA operation. The earlier enemy systems and characteristics can be identified, the more effective are the measures that can be conducted against them.

According to [15], FMCW radar incorporating a frequency hopping spread spectrum (FHSS) technique is currently under development. Such a system has the merits of FMCW radar as well as the agility of a frequency hopping system, and will once again challenge the current ES and EA technologies. To operate against a FMCW-FHSS system, the need for repeater jammer incorporating smart jamming techniques can be expected. As new technology being developed overtime, the race of ES and EA against emitter EP technologies will continue.

The next chapter concludes the thesis project. The results from both LVRTS experiment and MATLAB simulation are summarized. A brief discussion on modifying the simulation model for extended testing is also provided. In order to enhance the effectiveness of overall EA operation against FMCW radar, future studies on improving ES capability are suggested.

VII. CONCLUSION

To study the subject of FMCW radar jamming, this research has taken three different approaches, including theoretical studies, hardware experiment and computer simulation. From the collective result of all three approaches, the thesis project can offer these conclusions:

As other studies suggested, FMCW radar DSP is unable to distinguish between the real radar echo signal and a jamming signal with identical modulation. In such case, the jamming signal receives the radar processing gain, which allows it to penetrate radar DSP and alter the detection result. This makes FMCW radar vulnerable to repeater jamming. Repeater jammer requires the victim radar parameters be available in the system database. So when the radar signal is detected, the DRFM technique generator has sufficient knowledge of the waveform to apply proper delay and Doppler shift. With proper design of the modulation parameters, a realistic false target that is capable of seducing both the radar range gate (RGPO) and velocity gate (VGPO) can be generated.

With sufficient PRF, the energy impulse provided by pulse jamming signal can significantly increase the JSR, given that the jamming bandwidth covers the radar passband. Since pulse jamming is non-coherent to the radar receiver, it receives much attenuation at the receiver DSP. Theoretically, the amount of attenuation depends on the modulation waveform of the pulse signal. If the jamming signal chirp rate is somewhat similar to the radar waveform, the jamming signal receives less attenuation, make EA more effective. The attenuation can be compensated by high jamming power if available. On the operation side, pulse jamming is a good option when radar passband is somewhat known. Pulse jamming also has the potential to “fry” the radar receiver circuit with a strong impulse. However, it is unlikely to happen to modern radar systems, as impulse protection circuits are usually implemented. Meanwhile, the modern missile seeker equipped with anti-radiation capability also reduces the effectiveness of noise jamming techniques.

Although the example in Chapter V suggests that random noise receives the most attenuation at radar mixer output, obvious jamming effect was observed in the LVRTS experiment. The result proves that the band-limited random noise jamming can also be effective against FMCW radar systems if the noise bandwidth is limited within the radar passband. As the noise energy injected to the radar receiver is the product of the noise power density and receiver bandwidth, the maximal jamming effect occurs when the noise bandwidth is equal to the receiver bandwidth. But when compared with other jamming techniques, it is not power efficient. However, when the radar operation frequency band is unknown, a broad-band random noise waveform may be the only option. As with the pulse jamming waveform, the noise waveform can attract anti-radiation seekers and jeopardize the EA system.

From the discussion above, it can be concluded that the effectiveness of jamming techniques highly depends on the information about the radar system available to the jammer. However, acquiring FMCW emitter parameters is difficult in the real-world EW scenario. The LPI characteristics allow the FMCW radar to operate below environment noise, especially in a battlefield, where radio spectrum is congested with signals of radars and communication systems from both friends and foes. As the amount of information that can be obtained by the ELINT operator determines the EA techniques to be deployed, battlefield intelligence providing enemy platform information becomes the key to a successful EA operation. Knowing the position, capability and mission of the victim emitter, an ELINT operator is more likely to extract suspicious signals among clutters, and possibly identify the parameters of the signal to be jammed. The network-centric EW operation is the modern approach for enhanced intelligence acquiring as well as command and control. In such case, information is exchanged and shared among sensors, shooters and commander via wideband network in a timely manner. The network-centric operation allows deployment of multiple UAVs to cover a wide-range of battlefield for intelligence. The collected data can then be analyzed for possible EA operation.

The simulation model of this research has the potential to be modified for more complicated testing. For example, by adding radar scan pattern and Markov Chain functions, a three-dimensional radar model can be constructed. In such case, the effect of

jamming signals to the target angle can be examined. Furthermore, a more complex EW scenario including factors of multiple targets, environment clutter and meteorology can also be modeled for more realistic simulation.

As this research has investigated the jamming phase of EA operation against FMCW, future studies on improving ELINT capability in identifying LPI radar is suggested. In LPI signal analysis, Wigner-Ville Distribution, Choi-Williams Distribution, Quadrature Mirror Filtering and Cyclostationary Spectral Analysis are popular algorithms that are implemented in modern ES system to visualize the signal parameters in time-versus-frequency domain. However, when an LPI transmission is intercepted, the radar parameter is interpreted and cross-referenced visually by ELINT operators among different algorithms. The efficiency of this process highly depends on the skill and experience of the ELINT operators. In modern warfare where time and precision are critical factors, a poor ELINT operator can not only reduce EA effectiveness, but also endanger entire operation. Therefore, a computer algorithm that can automatically and accurately interpret the signal parameters can significantly improve the signal identification and classification process hence benefits the entire EA operation.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] P. E. Pace, *Detecting and Classifying Low Probability of Intercept Radar* (2nd ed.). Norwood, MA: Artech House, 2009.

[2] D. L. Adamy, *EW 101: A First Course in Electronic Warfare.* Norwood, MA: Artech House, 2001.

[3] J. S. Fu and Y. Ke. "Anti-jamming aspects of linear FM and phase coded pulse compression by simulation," *CIE International Conference of Radar Proc.,* Beijing, 1996, pp. 605–608.

[4] W. K. McRitchie and S. E. McDonald. (1999, Mar). Detection and jamming of LPI radars. Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/zbd87/p514732.pdf

[5] B. Mullarkey, The differences between pulse radar and FMCW ones. Available: http://www.navigate-us.com/files/uploads/file/Review_5_Radar-1-1.pdf

[6] T. Venkatamuni, L. S.Sudhakara Sarma, A.T.Kalghatgi, "Adaptive reflected power canceller for single antenna FMCW radar," *Microwave Conf.*, Singapore, APMC, 2009, pp. 1841-1844.

[7] P. E. Pace and L. L. Taylor, "False alarm analysis of the envelope detection GO-CFAR processor," in *Proc. IEEE Aerosp. Electron. Syst. Mag*., vol. 30, no.3, pp. 848-864, Jul, 1994.

[8] T. Van Cao, "A CFAR algorithm for radar detection under severe interference," *Proc. 2004 Intelligent Sensors, Sensor Networks and Information Processing Conf.*, Melbourne, ISSNIP. Australia, 2004, pp. 167–172.

[9] Lab-Volt (Quebec) Ltd., *Principles of Radar Systems Student Manual*. Telecommunications Radar, 2006.

[10] O. C. Mayhew, "Radar system characterization extended to hardware-in-the-loop simulation for the Lab-Volt™ Training System," M.S. thesis, Dept. Elect. Eng., Air Force Inst. of Technology, Dayton, OH, 2007.

[11] K. N. Parrish, An overview of FMCW systems in MATLAB. Available: http://www.cerc.utexas.edu/~kparrish/class/radar.pdf

[12] S. Hakin, M. Moher, *Introduction to Analog and Digital Communications*. Hoboken, NJ: John Wiley & Sons, 2007.

[13] R.G. Lyons, *Understanding Digital Signal Processing* (3rd ed.). Boston, MA: Pearson Education, 2011.

[14] D. C. Schleher, *Electronic Warfare in the Information Age.* Norwood, MA: Artech House, 1999.

[15] A. B. Suksmono, Development of FMCW-FHSS spread-spectrum radar for defense applications. Available: http://www.lppm.itb.ac.id/research/?p=976

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California